DRAFT

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

Version 1.0

July 1, 2020

FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
7/1/2020	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 alone. 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 National Institute of Standards and Technology (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.

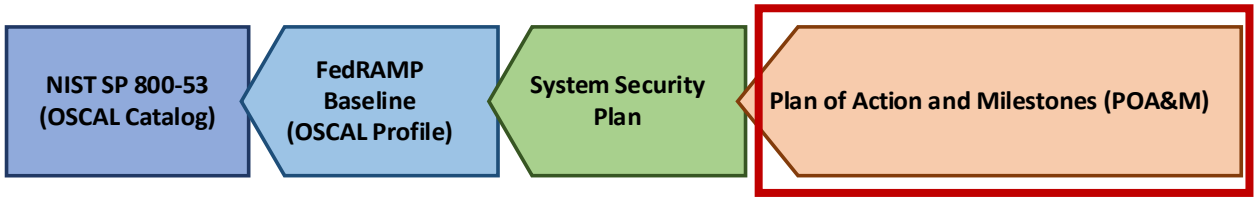
3.1. XML and JSON Formats

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.

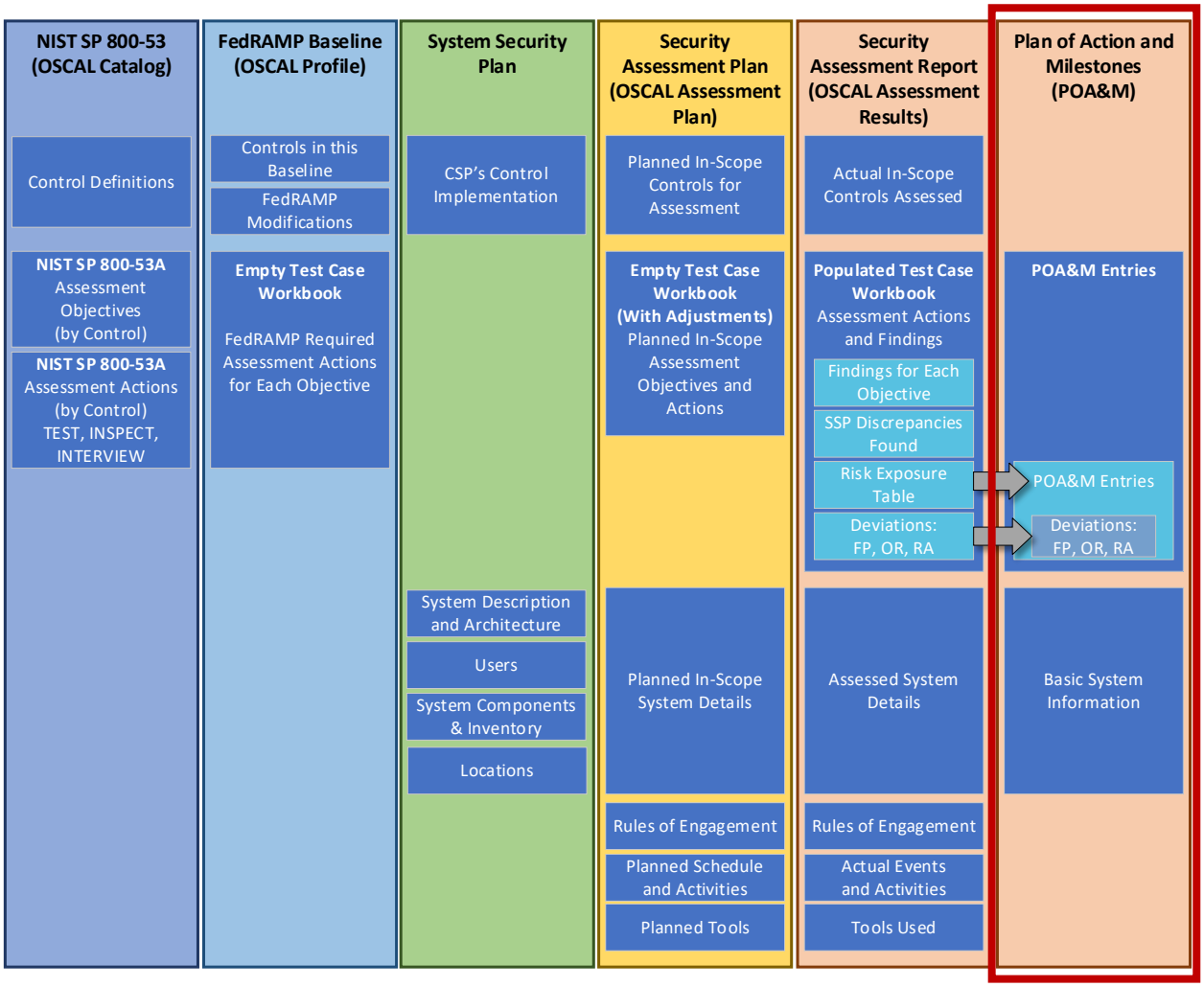
3.2. POA&M File Concepts

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 for information such as system description, boundary, users, locations, and inventory items.

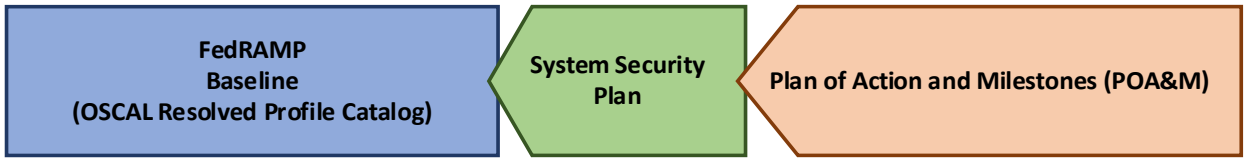
The POA&M also inherits the SSP's pointer to the appropriate OSCAL-based FedRAMP Baseline. Through that linkage, the POA&M references the control baseline definitions for the system's baseline.

3.2.1. Resolved Profile Catalogs

The resolved profile catalog for each FedRAMP baseline is a pre-processing the profile and catalog to produce the resulting data. This reduces 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.

Developers should be aware that 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.



The Resolved Profile Catalog for each FedRAMP Baseline reduces tool processing

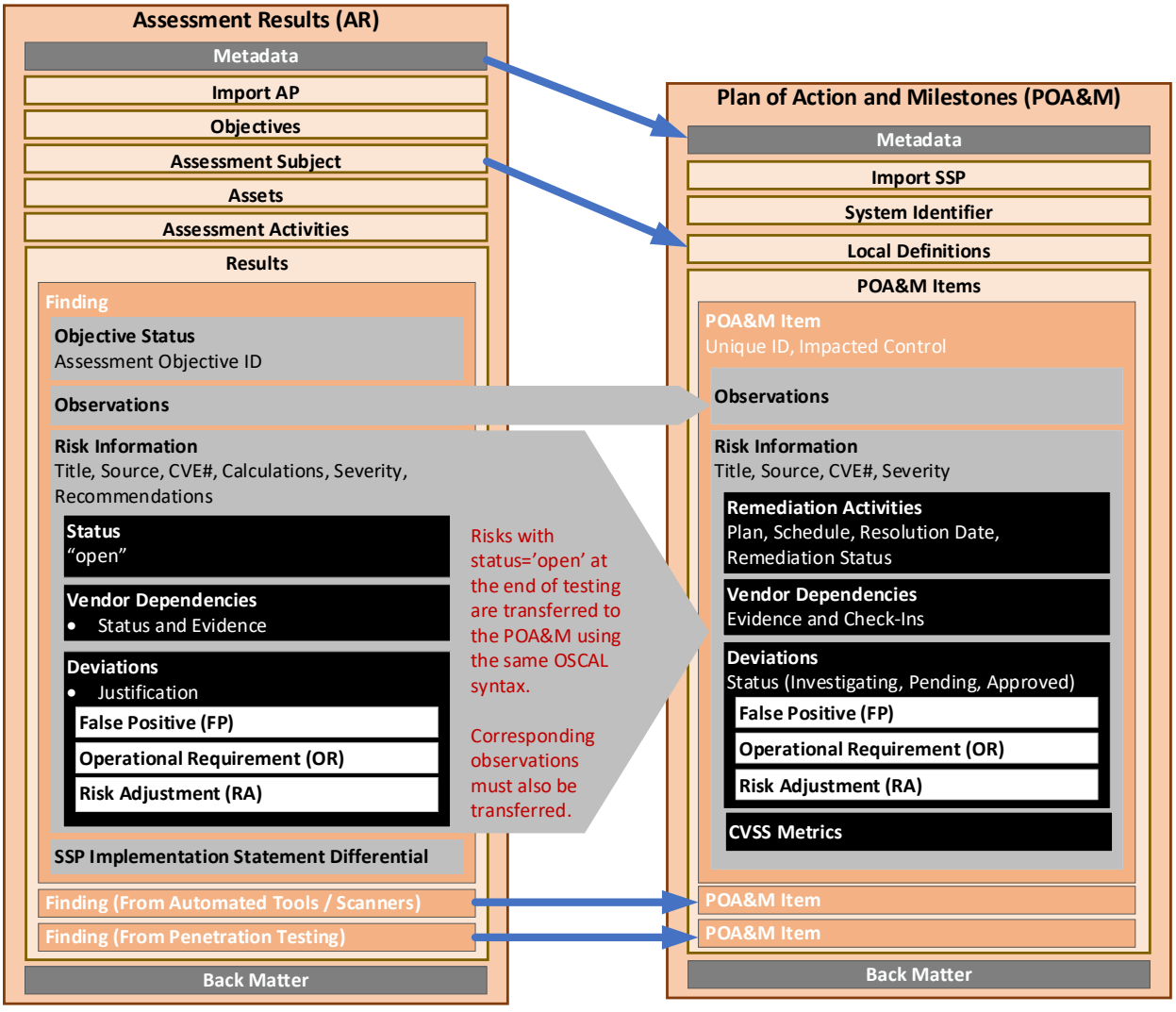
For more information about resolved profile catalogs, see the *Guide to OSCAL-based FedRAMP Content Appendix C, Profile Resolution*.

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

FedRAMP requires residual risks from an initial or annual SAR to be reflected in the POA&M. The `findings` assembly of an OSCAL-based SAR uses the same syntax as the `poam-item` assembly of an OSCAL based POA&M to enable easy transfer of residual risk information into the POA&M.

A tool should extract the entire **`findings`** assembly for any finding that has a `risk` assembly with the `risk-status` field set to "`open`". The tool may drop the objective-status assembly from the finding assembly. The tool may also drop the `assessor` and `relevant-evidence` assemblies from any `observation` assemblies. Finally, the tool should ensure any remaining ID or UUID values are addressable - either within the linked SSP or by duplicating any related `party`, `resource` or `local-definition` content from the SAP or SAR 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.



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

3.3. OSCAL-based FedRAMP POA&M Template

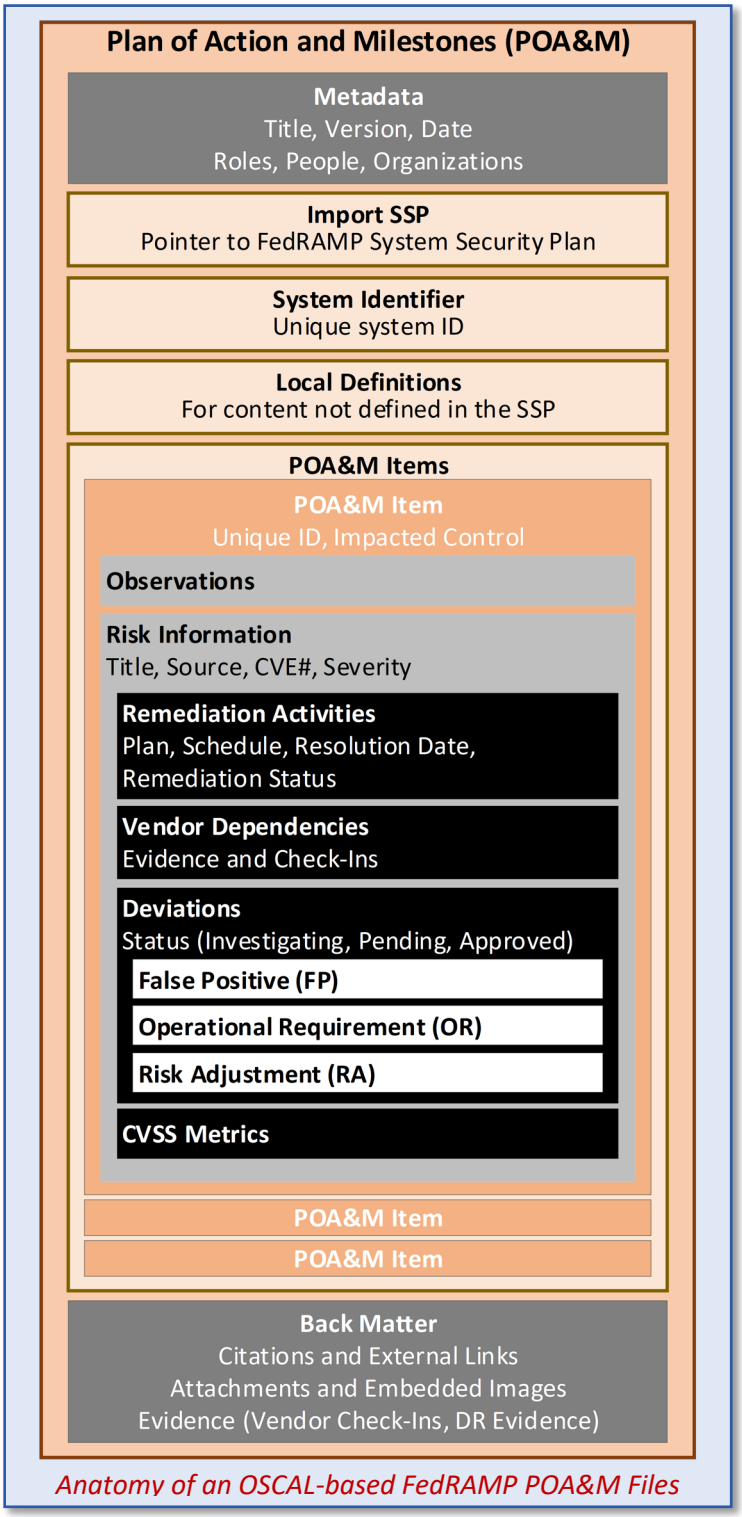
FedRAMP offers an OSCAL-based POA&M shell file in both XML and JSON formats. This shell contains many of the FedRAMP required standards to help get you started. This document is intended to work in concert with that file. The OSCAL-based FedRAMP POA&M Template is available in XML and JSON formats here:

- 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 POA&M Model syntax found here:

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



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.
- **POA&M Items**: Enumerates each individual POA&M item. 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 circumstances, FedRAMP enables critical SSP content to be defined within the OSCAL-based POA&M.

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="../ssp/FedRAMP-SSP-OSCAL-File.xml" />

- OR -

   <import-ssp href="#[uuid-value]" />
```

XPath Queries

```
(POA&M) URI to SSP:
  /*/import-ssp/@href
```

If the value is a URI fragment, such as `#96445439-6ce1-4e22-beae-aa72cfe173d0`, the value to the right of the hashtag (#) is the UUID value of a resource in the SAP 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.

POA&M Back Matter Representation

```
<back-matter>
   <resource uuid="96445439-6ce1-4e22-beae-aa72cfe173d0">
      <title>[System Name] [FIPS-199 Level] SSP</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">ssp</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" />
      <!-- Do not embed a Base64-encoded SSP. -->
   </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

```
(POA&M) Referenced OSCAL-based SSP

XML:
  /*/back-matter/resource[@uuid='96445439-6ce1-4e22-beae-aa72cfe173d0']
  /rlink[@media-type='application/xml']/@href

OR JSON:
  /*/back-matter/resource[@uuid='96445439-6ce1-4e22-beae-aa72cfe173d0']
  /rlink[@media-type='application/json']/@href
```

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

The OSCAL-based POA&M must always have an `import-ssp` field. If no OSCAL-based SSP exists, 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="#7c30125f-c056-4888-9f1a-7ed1b6a1b638" />

<back-matter>
   <resource id="7c30125f-c056-4888-9f1a-7ed1b6a1b638">
      <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']/..
```

3.5.2. System Inventory

With OSCAL, the system inventory is intended to exist as `component` and `inventory-item` assemblies in the `system-implementation` assembly of an OSCAL-based SSP. The OSCAL-based POA&M is designed to cite the UUID for each system inventory assets normally listed in the Asset Identifier column of the MS Excel-based template.

When considering system-inventory in the context of a POA&M, there are three important scenarios to consider:

- **Scenario 1: Both an OSCAL-based SSP and an OSCAL-based POA&M exist, and are delivered together**: This is typical for initial and annual assessments.
- **Scenario 2: Both an OSCAL-based SSP and an OSCAL-based POA&M exist, but the POA&M is delivered without the SSP**: This is typical for monthly continuous monitoring (ConMon) deliveries.
- **Scenario 3: No OSCAL-based SSP exists, yet an OSCAL-based POA&M exists**: This scenario may exist if a CSP has adopted OSCAL for continuous monitoring, but has not yet adopted OSCAL for SSP content.

The Asset Identifier column simply cites UUID values for components and inventory items the same for all three scenarios; however, the system inventory itself must be handled differently for each scenario.

Scenario 1: Both an OSCAL-based SSP and an OSCAL-based POA&M exist, and are delivered together

When the OSCAL-based SSP and POA&M both exist and are delivered together, no additional action is necessary. Within the POA&M, any references to assets from within the Asset Identifier column uses the UUID of the component or inventory-item in the SSP. All details about the asset remain in the SSP.

Scenario 2: Both an OSCAL-based SSP and an OSCAL-based POA&M exist, but the POA&M is delivered without the SSP

When the OSCAL-based SSP exists, but is not delivered with the OSCAL-based POA&M, the CSP's POA&M tool must duplicate all `component` and `inventory-item` assemblies from the `system-implementation` assembly of the SSP to the `local-definitions` assembly of the POA&M. The UUID values may remain the same as part of the duplication.

Any `role`, `party`, or `resource` cited by a `component` or `inventory-item` assembly must also be duplicated to the POA&M in the appropriate section. For example, if an administrator for a component is identified using a `party-uuid`, the `party` assembly must be duplicated from the SSP's `metadata` assembly to the POA&M's `metadata` assembly.

The syntax for `component` and `inventory-item` assemblies in local-definitions is identical to the syntax in the SSP as described in the *Guide to OSCAL-based System Security Plans (SSP)*.

Scenario 3: No OSCAL-based SSP exists, yet an OSCAL-based POA&M exists

If no OSCAL-based SSP exists, the system inventory must be defined fully in the local-definitions assembly of the POA&M using the same component and inventory-item syntax described in the *Guide to OSCAL-based System Security Plans (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* , 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
- Local definitions; and
- POA&M Items syntax. Individual POA&M item syntax is the same as the Findings syntax in the SAR.

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 adds details that are unique to the POA&M.

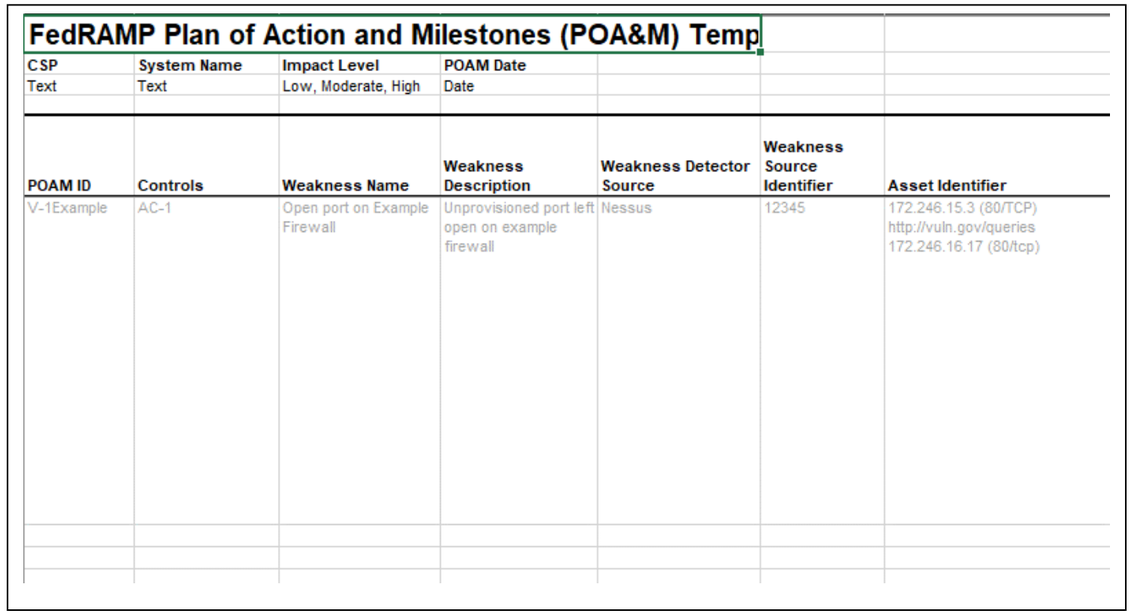
4.1. Representing the POA&M

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 4.6*
Document Approvers	*Guide to OSCAL-based FedRAMP Content, Section 4.7*
Acronyms and Glossary	*Guide to OSCAL-based FedRAMP Content, Section 4.8*
Laws, Regulations, Standards and Guidance	*Guide to OSCAL-based FedRAMP Content, Section 4.9*
Attachments and Citations	*Guide to OSCAL-based FedRAMP Content, Section 4.10*

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



FedRAMP Plan of Action and Milestones (POA&M) Temp

CSP	System Name	Impact Level	POAM Date
Text	Text	Low, Moderate, High	Date

POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detector Source	Weakness Source Identifier	Asset Identifier
V-1Example	AC-1	Open port on Example Firewall	Unprovisioned port left open on example firewall	Nessus	12345	172.246.15.3 (80/TCP) http://vuln.gov/queries 172.246.16.17 (80/tcp)

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

4.2. Individual POA&M Entries

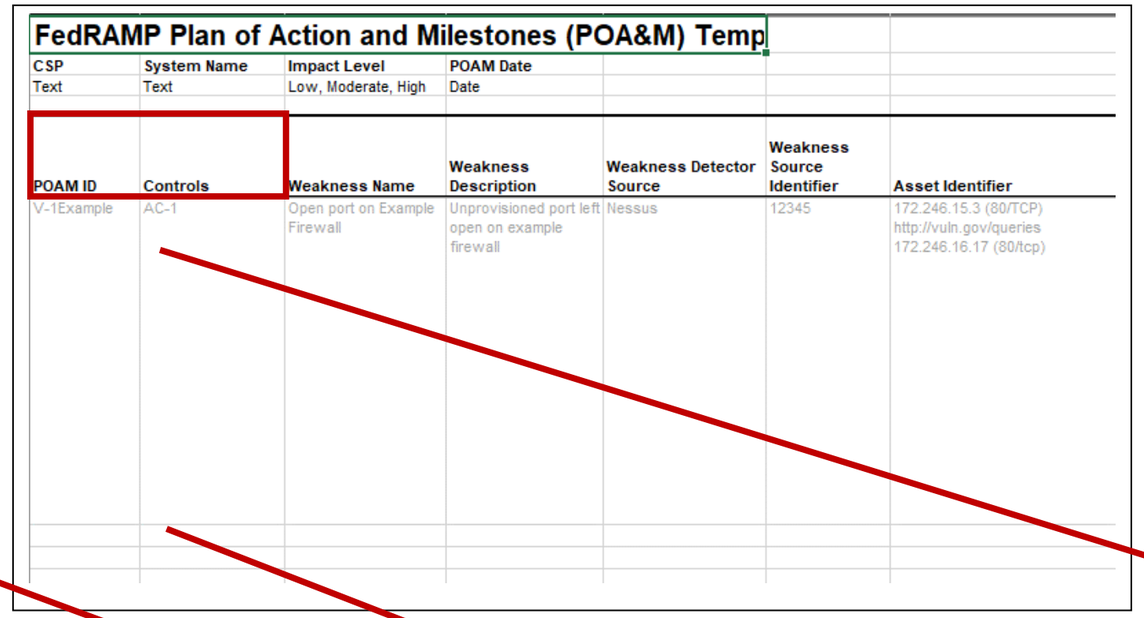
An entire OSCAL-based POA&M has exactly one `poam-items` assembly, containing all POA&M entries. Each POA&M entry is a `poam-item` within the `poam-items` assembly. For those familiar with using the Excel-based FedRAMP POA&M template, each row in the spreadsheet is represented by a single `poam-item` assembly.

OSCAL requires the `poam-items` assembly to include `title`, `description`, `start` and `end` fields. The value of the `title` and `description` fields may be anything the CSP feels is appropriate. FedRAMP suggests duplicating the `title` value used in the `metadata` section.

A POA&M tool should set the `start` field to reflect the `date-time-stamp` value of the earliest finding. The end field should reflect the effective-date of the POA&M content. For example, if the POA&M content was updated Monday the 8th based on data provided as of Friday the 5th, the modified field in the metadata section will reflect Monday the 8th; however, the end field in the `poam-items` assembly must reflect Friday the 5th.

Representation

```
   <metadata>
      <title>[System Name] FedRAMP Plan of Action and Milestones (POA&amp;amp;M)</title>
      <last-modified>2020-06-01T00:00:00Z</last-modified>
      <version>0.0.0</version>
      <oscal-version>1.0.0-milestone3</oscal-version>
      <!-- role, location, party, responsible-party -->
   </metadata>

   <!-- import -->
   <!-- local-definitions -->
   <poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
      <title>Current POA&amp;amp;M Items</title>
      <description>
         <p>These are the current POA&amp;amp;M items for this system.</p>
      </description>
      <start>2018-04-14T00:00:00.0Z</start>
      <end>2020-06-05T00:00:00.0Z</end>

      <!-- poam-item (spreadsheet row 1) -->

      <!-- poam-item (spreadsheet row 2) -->

      <!-- poam-item(spreadsheet row 3) -->

   </poam-items>

   <!-- back-matter -->
```



FedRAMP Plan of Action and Milestones (POA&M) Temp

CSP	System Name	Impact Level	POAM Date
Text	Text	Low, Moderate, High	Date

POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detector Source	Weakness Source Identifier	Asset Identifier
V-1Example	AC-1	Open port on Example Firewall	Unprovisioned port left open on example firewall	Nessus	12345	172.246.15.3 (80/TCP) http://vuln.gov/queries 172.246.16.17 (80/tcp)

4.2.1. Individual POA&M Entries: Findings

As with the Excel-based POA&M template, there is typically a single `poam-item` for each unique vulnerability, and all impacted hosts are identified within. On occasion, the CSP intends to remediate hosts in sub-groups. In this instance, the unique vulnerability may be split into multiple finding assemblies. Each would contain a sub-group of hosts to be addressed. This is analogous to entering the same unique vulnerability on multiple rows of the Excel-based POA&M template for the same reason.

Whether a single finding assembly or multiple groups, the same guidance applies. Within each `finding` assembly, the `title` field must reflect the identified vulnerability as provided by the scanning tool.

OSCAL syntax requires a description field; however, FedRAMP does not expect content here. It may remain empty.

The CSP-assigned unique POA&M ID must be present using the FedRAMP extension, "POAM-ID".

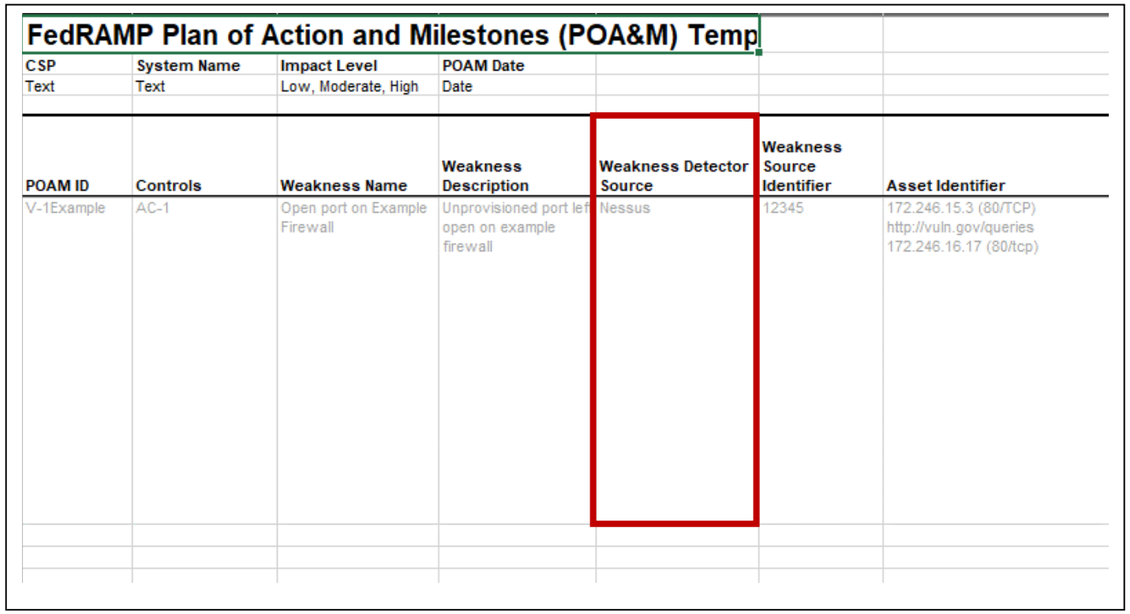
Each impacted control must be identified using the FedRAMP extension, "`impacted-control-id`". The value must be the ID of the impacted control as it appears in the appropriate FedRAMP baseline (OSCAL profile). One entry per control.

The `date-time-stamp` field must be set to the Original Detection Date, which may be the tool's timestamp.

Within the `poam-item` assembly, there must be exactly one `observation` assembly, and exactly one `risk` assembly.

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->

   <poam-item uuid="0be71cd3-f850-47db-836f-14511edbd90e">
      <title>[EXAMPLE]POA&amp;M Item</title>
      <description/>
      <prop name="POAM-ID" ns="https://fedramp.gov/ns/oscal">V-1</prop>
      <prop name="impacted=control-id" ns="https://fedramp.gov/ns/oscal">ac-2</prop>
      <prop name="impacted=control-id" ns="https://fedramp.gov/ns/oscal">ac-2.1</prop>
      <date-time-stamp>2020-06-01T00:00:00Z</date-time-stamp>

      <observation uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab">
         <!-- cut -->
      </observation>

      <risk uuid="9cbd98f3-abcb-4948-ad06-14e0bcba742f">
         <!-- cut -->
      </risk>
   </poam-item>

   <!-- poam-tem -->
      <!-- observation -->
      <!-- risk -->

   <!-- poam-item -->
      <!-- observation -->
      <!-- risk -->

</poam-items>
```



FedRAMP Plan of Action and Milestones (POA&M) Temp

CSP	System Name	Impact Level	POAM Date
Text	Text	Low, Moderate, High	Date

POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detector Source	Weakness Source Identifier	Asset Identifier
V-1Example	AC-1	Open port on Example Firewall	Unprovisioned port left open on example firewall	Nessus	12345	172.246.15.3 (80/TCP) http://vuln.gov/queries 172.246.16.17 (80/tcp)

4.2.2. Individual POA&M Entries: Observations

Within the `observation` assembly, the `observation-method` field must be set to "`TEST`" for scanning results. Set this value to "`TEST`", "`EXAMINE`" or "`INTERVIEW`" as appropriate for risks identified by other means.

The `observation-type` field must be set to "`finding`".

The `uuid` flag of the `origin` field must identify the Weakness Detector Source of the information. For monthly scanning, this must identify the automated tool's UUID, and the `type` flag must be set to "`tool`".

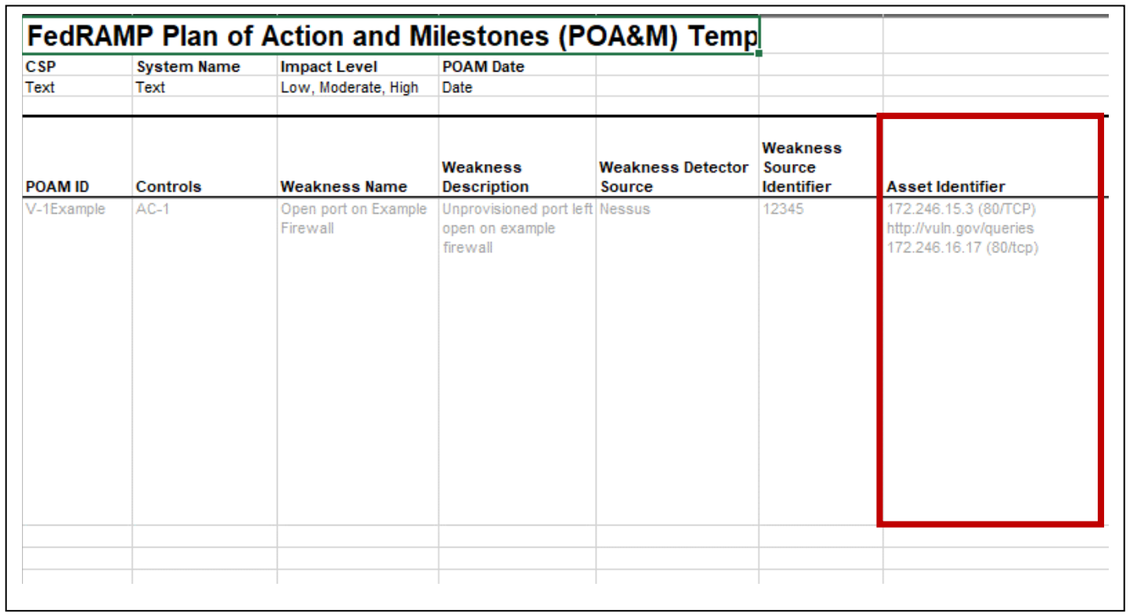
> The tool must be defined as a `component` in the `local-definitions` assembly, using the same syntax and approach described in the *Guide to OSCAL-based Security Assessment Plans (SAP)*, *Section 4.14, SAP Test Plan: Testing Performed Using Automated Tools*. If the POA&M item was identified another way, the local-definitions assembly should have

The `href` flag in the `relevant-evidence` field must point to the `resource` containing the raw tool output attached in the back-matter using a URI fragment. Relevant evidence information is encouraged, but not required for POA&M entries.

At the end of the `findings` assembly, the UUID for the operator of the scanning tool may be listed as the `party-uuid` for the finding. There may be more than one. Each `party-uuid` must reference a `party` assembly in either the POA&M's `metadata` section, or the `metadata` section of the imported SSP. Tool operator information is optional, but a POA&M tool should display the party information if one or more `party-uuid` fields are present.

Representation

```
   <local-definitions>
      <component uuid="9d194268-a9d1-4c38-839f-9c4aa57bf71e" component-type="software">
         <title>XYZ Vulnerability Scanning Tool</title>
         <description/>
         <prop name="vendor">Vendor Name</prop>
         <prop name="name">Tool Name</prop>
         <prop name="version">1.2.3</prop>
         <status state="operational"/>
      </component>
   </local-definitions>

   <poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
      <!-- title, description, start, end -->
      <poam-itemuuid="0be71cd3-f850-47db-836f-14511edbd90e">
         <!-- title, description, POA&M ID, date-time-stamp -->
         <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
            <description />
            <observation-method>TEST</observation-method>
            <observation-type>finding</observation-type>

            <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>
      </poam-item>
   </poam-items>
```



FedRAMP Plan of Action and Milestones (POA&M) Temp

CSP	System Name	Impact Level	POAM Date
Text	Text	Low, Moderate, High	Date

POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detector Source	Weakness Source Identifier	Asset Identifier
V-1Example	AC-1	Open port on Example Firewall	Unprovisioned port left open on example firewall	Nessus	12345	172.246.15.3 (80/TCP) http://vuln.gov/queries 172.246.16.17 (80/tcp)

System Inventory

When providing a monthly POA&M to FedRAMP using OSCAL, the OSCAL-based inventory may be delivered either:

- by delivering the entire OSCAL-based SSP file, including the latest system inventory; or
- by duplicating all `component` and `inventory-item` assemblies from the `system-implementation` assembly of the SSP to the `local-definitions` assembly of the POA&M.

See *Section 3.5.2, System Inventory* for more information.

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

4.2.3. Individual POA&M Entries: Asset Identifiers

For scanner tool findings, impacted assets are identified using the `subject-reference` field. One field for each impacted asset. The `type` flag should be set to either "`inventory-item`" or "`component`".

The `uuid-ref` flag must point to an inventory item or component defined in the SSP inventory or POA&M local-definitions.

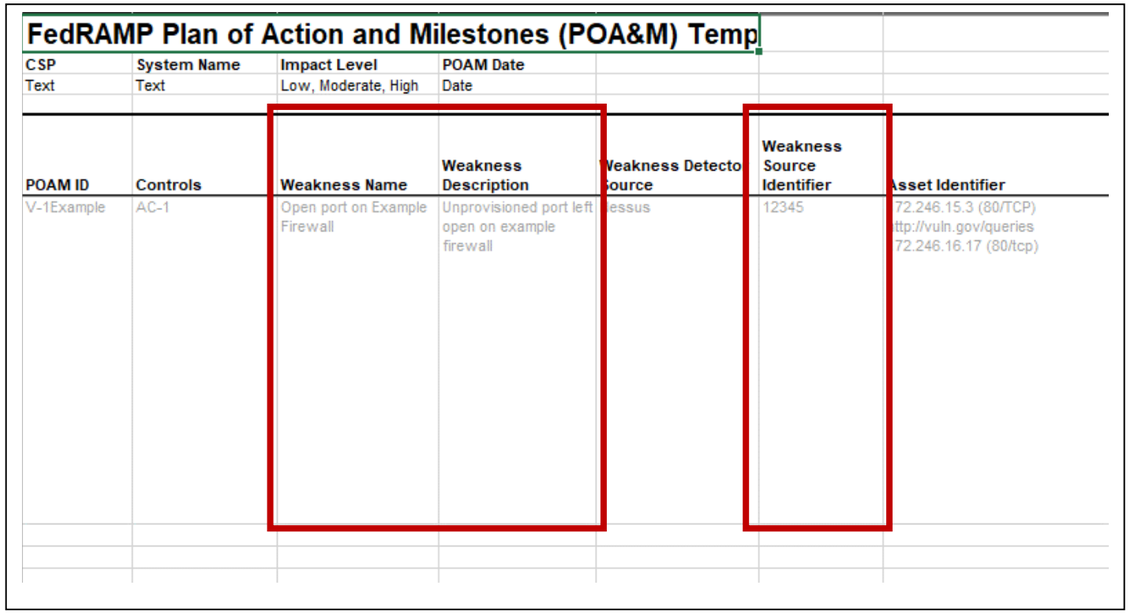
When providing a monthly POA&M to FedRAMP using OSCAL, the based inventory may be delivered either by:

- delivering the entire OSCAL-based SSP file, including the latest system inventory; or
- duplicating all `component` and `inventory-item` assemblies from the `system-implementation` assembly of the SSP to the `local-definitions` assembly of the POA&M. Any `role` or `party` citations in this content must also be duplicated from the SSP `metadata` assembly to the POA&M `metadata` assembly.

All details about the asset become available as a result of that UUID reference, such as IP address, fully qualified domain name (FQDN), and the asset's point of contact.

Representation

```
<local-definitions>
   <!-- component and inventory-item assemblies not used when delivering SSP -->
   <component uuid="a49ed61e-fca1-4ffa-b5e7-c23a2375a7a0" component-type="virtual">
      <title>Component Definition</title>
      <description>
         <p>A virtual component.</p>
      </description>
      <prop name="os-name">Linux Flavor</prop>
      <prop name="os-version">1.2.0</prop>
      <status state="operational"></status>
   </component>
   <inventory-item uuid="deb26a75-6d97-4811-ae0e-ae1c710366c1" asset-id="">
      <description><p>An instance of the above component.</p></description>
      <prop name="ipv4-address">10.10.10.10</prop>
      <prop name="fqdn">host.domain.cloud</prop>
      <implemented-component component-id="a49ed61e-fca1-4ffa-b5e7-c23a2375a7a0"
                                                                  use="runs-software" />
   </inventory-item>
</local-definitions>

<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="0be71cd3-f850-47db-836f-14511edbd90e">
      <!-- title, description, POA&M ID, date-time-stamp -->
      <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
         <!-- description, observation-method, observation-type -->

         <subject-reference type="inventory-item"
                            uuid-ref="deb26a75-6d97-4811-ae0e-ae1c710366c1" />
         <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, relevant-evidence -->
      </observation>
      <!-- risk -->
   </poam-item>
</poam-items>
```



FedRAMP Plan of Action and Milestones (POA&M) Temp

CSP	System Name	Impact Level	POAM Date				
Text	Text	Low, Moderate, High	Date				
POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detecto Source	Weakness Source Identifier	Asset Identifier	
V-1Example	AC-1	Open port on Example Firewall	Unprovisioned port left open on example firewall	Nessus	12345	72.246.15.3 (80/TCP) http://vuln.gov/queries 72.246.16.17 (80/tcp)	

Risk Metric Fields

The `risk metric` fields are designed to allow risk values and identifiers from different frameworks, systems, and tools to co-exist in the same `risk` assembly. For example, a scanning tool may provide risk values assigned by the tool itself, as well as a CVE identifier, IAVM severity score, and CVSS metrics. The system may also be subject to multiple frameworks using different risk score values or risk calculation methods.

See the *Risk Metrics* tab of the *FedRAMP OSCAL Registry* for a comprehensive list of risk metric `name`, `class`, and `system` flags, and associated accepted values.

Common values for the `system` flag include:

- `https://fedramp.gov`
- `iavm`
- `cve`
- `CVSSv2, CVSSv3, CVSSv3.1`

For scanner-specific values, FedRAMP requires the POA&M tool consistently apply the same system value to all risk-metrics from a given tool. Until risk-metric systems can be more formally identified for individual tools, FedRAMP recommends the POA&M tool use the UUID of the scanning tool associated with its `component` definition in the `local-definitions` assembly, as assigned in *Section 4.2.2, Individual POA&M Entries: Weakness Information*.

The `description` and `risk-statement` 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

4.2.4. Individual POA&M Entries: Weakness Information

Weakness details are identified in the `risk` assembly.

The Weakness Name appears in the `title` field, and the Weakness Description appears in the `description` field.

The Weakness Source Identifier is provided using a `risk-metric` field with the `name` flag set to "`vulnerability-id`" and the `system` flag set to the UUID of the scanning tool as assigned in *Section 4.2.2, Individual POA&M Entries: Weakness Information*.

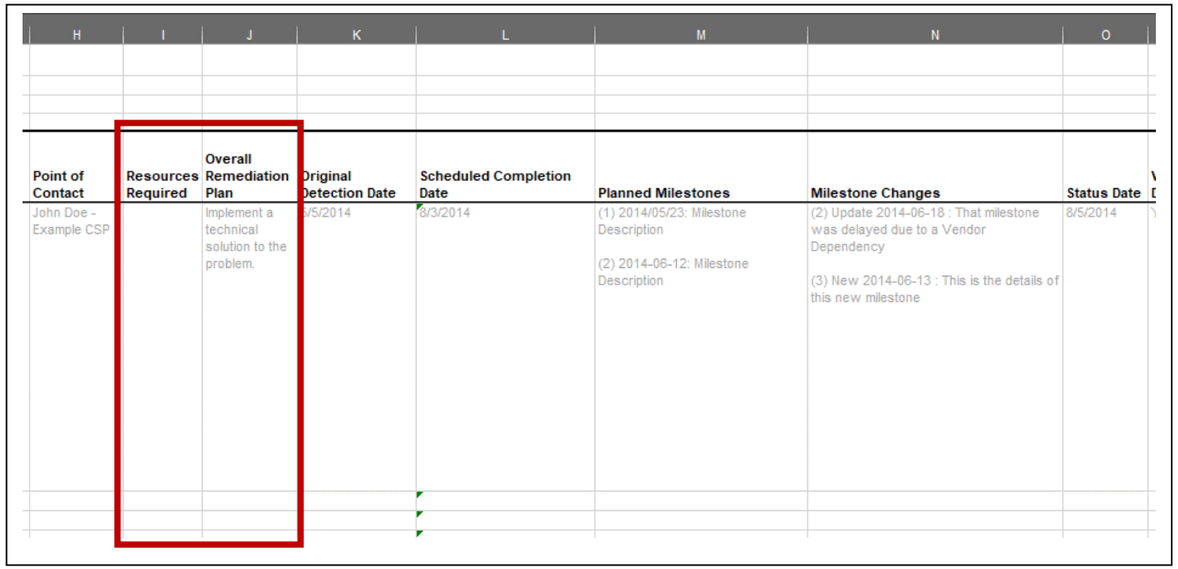
Other scanner-tool provided values may be reflected using additional risk metrics using the same system value as above.

When the scanner tool provides risk values from other recognized systems, such as a CVE number, IAVAM severity, or CCSV metric, the risk-metric field should reflect the original system. For example, if the scanner tool provides a CVE number, the `risk-metric` field's `system` flag should reflect "`cve`" as the system, not the scanner tool.

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.

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="170dd310-1a92-4fcf-a12b-ebfa03d9e6d8">
      <!-- title, description, date-time-stamp -->
      <!-- observation: Weakness Detector Source, Asset Identifiers -->
      <risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
         <title>Weakness Name</title>
         <description>
            <p>This is the Weakness Description.</p>
         </description>

         <risk-metric name="vulnerability-id"
                      system="uuid-of-scanner tool">VulID-001</risk-metric>
         <risk-metric name="plugin-id"
                      system="uuid-of-scanner tool">Plugin-ID</risk-metric>
         <risk-metric name="iavm-severity"
                      system="uuid-of-scanner tool">high</risk-metric>

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

         <risk-metric name="impact"     class="initial"
                      system="scanner-name">high</risk-metric>
         <risk-metric name="likelihood" class='initial'
                      system="https://fedramp.gov">high</risk-metric>
         <risk-metric name="impact"     class='initial'
                      system="https://fedramp.gov">high</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>
   </poam-item>
</poam-items>
```



Point of Contact	Resources Required	Overall Remediation Plan	Original Detection Date	Scheduled Completion Date	Planned Milestones	Milestone Changes	Status Date
John Doe - Example CSP		Implement a technical solution to the problem.	8/5/2014	8/3/2014	(1) 2014/05/23: Milestone Description (2) 2014-06-12: Milestone Description	(2) Update 2014-06-18 : That milestone was delayed due to a Vendor Dependency (3) New 2014-06-13 : This is the details of this new milestone	8/5/2014

Accepted Values

- The `type` flag on the `remediation` field:
  - **recommendation**
  - **planned**
  - **final**
- The `type` flag on the `recommendation-origin` field :
  - **party**
  - **tool**
- The `type` flag on the `subject-reference` field :
  - **party**
  - **component**
  - **inventory-item**
  - **location**
  - **user**
  - **resource**

4.3. Recommended and Planned Remediation

Within the `risk` assembly, there must be a `remediation` assembly containing the tool's recommended mitigation. The `type` flag must be set to "`recommendation`". The `recommendation-origin` field's type flag must be set to "`tool`", and the `uuid-ref` must contain the UUID of the tool that generated the recommendation.

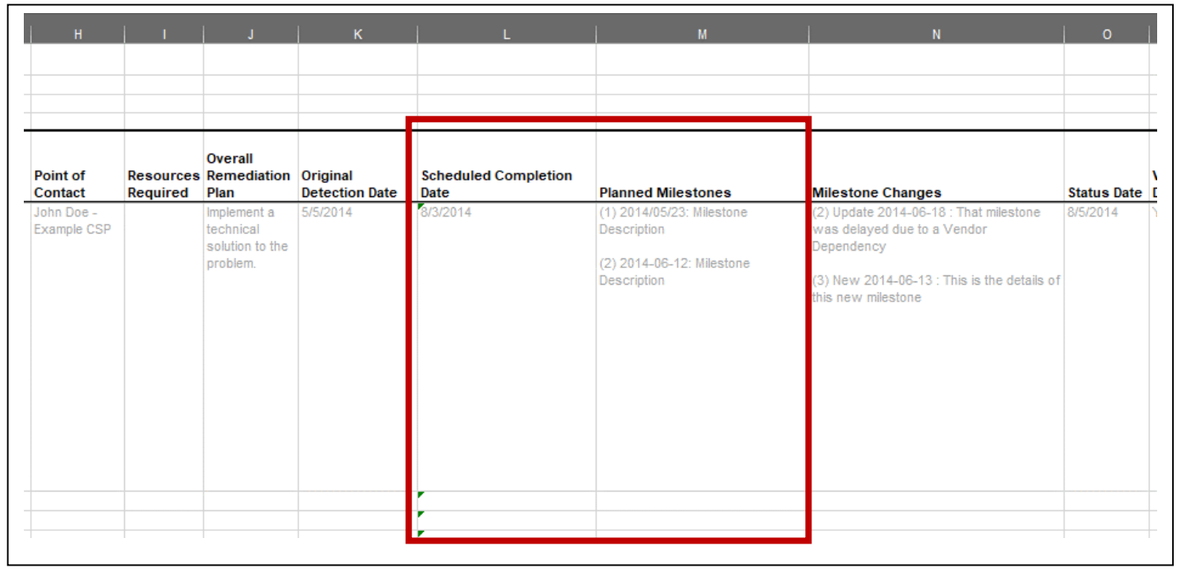
There must also be a `remediation` assembly containing the CSP's intended mitigation plan. The `type` flag must be set to "`planned`". The `recommendation-origin` field's type flag must be set to "`party`", and the `uuid-ref` must contain the UUID of either the CSP organization itself or the individual overseeing the activities, such as the ISSO.

"Resources Required" are identified within "planned" `remediation` assembly using the `required` assembly. Use the `description` field for a free-form explanation of required resources. Use one or more `subject-reference` fields to link to a specific party, component, inventory-item, system user, or resource. A combination of `description` and `subject-reference` fields may be used together.

Additional remediation recommendations may also be present, such as the assessor's recommendation copied from the SAR.

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->
      <!-- observation -->
      <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
         <!-- title, description, likelihood, impact, risk-statement -->

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

         <remediation uuid="9c3be116-9be2-4e34-b9ce-4f2b49975133"
                                                          type="planned">
            <title>CSP's Intended Remediation</title>
            <description>
               <p>A description of the Intended Remediation.</p>
            </description>
            <recommendation-origin type="party"
                                   uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
            <required uuid="7bd1a61e-4fda-4c52-a447-14072ef6e042">
               <subject-reference uuid-ref="6e0d71b5-3dac-4a9b-b60d-da61b95eccb9"
                                                                type="party" />
               <description><p>Describe required resources.</p></description>
            </required>
            <!-- schedule -->
         </remediation>
         <!-- risk-status -->
         <!-- remediation-tracking -->
      </risk>
   </poam-item>
</poam-items>
```



H	I	J	K	L	M	N	O
Point of Contact	**Resources Required**	**Overall Remediation Plan**	**Original Detection Date**	**Scheduled Completion Date**	**Planned Milestones**	**Milestone Changes**	**Status Date**
John Doe - Example CSP		Implement a technical solution to the problem.	5/5/2014	8/3/2014	(1) 2014/05/23: Milestone Description (2) 2014-06-12: Milestone Description	(2) Update 2014-06-18 : That milestone was delayed due to a Vendor Dependency (3) New 2014-06-13 : This is the details of this new milestone	8/5/2014

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

4.3.1. Planned Remediation Schedule

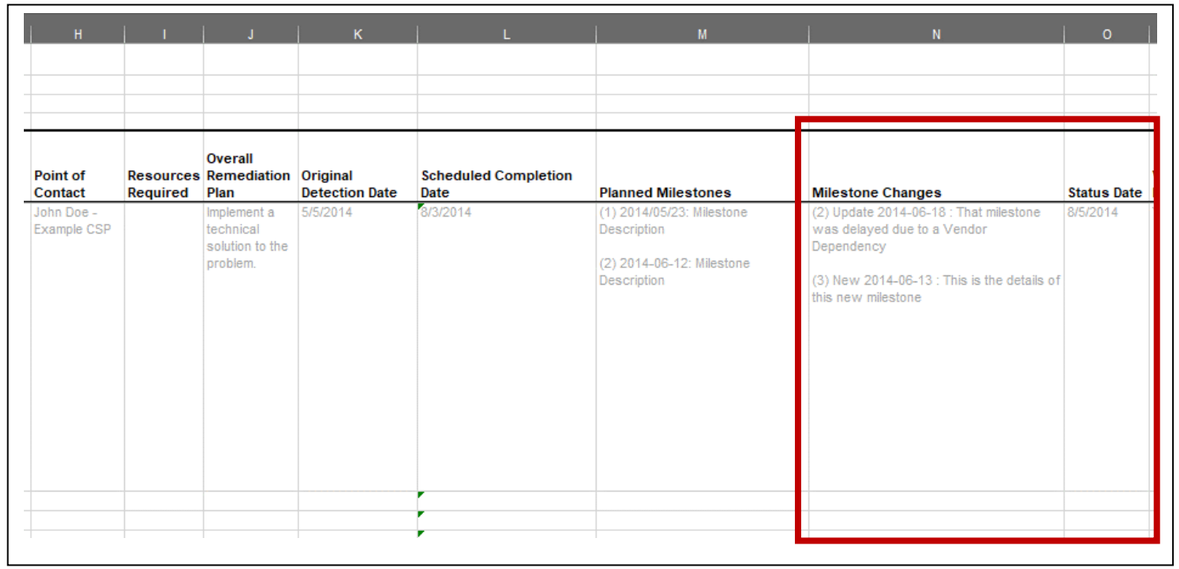
The Planned Milestones are identified within the `remediation` assembly using the `schedule` assembly.

The `schedule` assembly must include one or more `task` assemblies. Each `task` assembly must have a `title` field that briefly names the milestone, a `description` field, a `start` field and an `end` field. The `description` must be present, but may be empty.

The Scheduled Completion Date for the POA&M item is the value of the `end` field farthest in the future.

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->

      <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
         <!-- title, description, risk metrics, risk-statement -->

         <!-- remediation: tool recommendation -->

         <remediation uuid="752f9b0d-70ea-4576-98f7-fb3bb12524b9" type="planned">
            <title>CSP's Intended Remediation</title>
            <description>
               <p>A description of the Intended Remediation.</p>
            </description>
            <recommendation-origin type="party"
                                   uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
            <!-- required -->
            <schedule>
               <task uuid="a12dea1d-e4d1-4f09-aacf-1eaf203a3092">
                  <title>[Example]Activity 1</title>
                  <description><p>Optional description</p></description>
                  <start>2020-07-01T00:00:00Z</start>
                  <end>2020-07-02T00:00:00Z</end>
               </task>
               <task uuid="08c50f90-3b08-49fd-862d-32ec96e6bee5">
                  <title>[Example]Activity 2</title>
                  <description><p>Optional description</p></description>
                  <start>2020-07-05T00:00:00Z</start>
                  <end>2020-07-07T00:00:00Z</end>
               </task>
            </schedule>
         </remediation>

         <risk-status>open</risk-status>
         <!-- remediation-tracking -->
      </risk>
   <!-- party -->
   </poam-item>
</poam-items>
```



Point of Contact	Resources Required	Overall Remediation Plan	Original Detection Date	Scheduled Completion Date	Planned Milestones	Milestone Changes	Status Date
John Doe - Example CSP		Implement a technical solution to the problem.	5/5/2014	8/3/2014	(1) 2014/05/23: Milestone Description (2) 2014-06-12: Milestone Description	(2) Update 2014-06-18 : That milestone was delayed due to a Vendor Dependency (3) New 2014-06-13 : This is the details of this new milestone	8/5/2014

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

4.4. Risk Tracking

Tracking is initiated by adding the `remediation-tracking` assembly, which must have one or more `tracking-entry` assemblies. Each milestone change, vendor check-in, periodic status update, and action performed in the pursuit of remediating the risk are entered here as individual tracking entry updates.

Each `tracking-entry` assembly must have a `date-time-stamp`., `title`, and `description` field.

For performed actions, the `date-time-stamp` should reflect when the action was performed. For status updates, this should reflect the effective date of the status information.

The `title` field should match the `title` field in the `task` assembly's title when reporting the completion of a task in the schedule.

The `description` field must be present, but may be empty if appropriate.

If it is appropriate to attach evidence related to risk tracking, add an `observation` assembly with the appropriate evidence attached. If used, the `observation` assembly must have a `conformity` tag of "`risk-tracking`".

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->

      <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
         <!-- title, description, risk metrics, risk-statement -->

         <!-- remediation: tool recommendation -->
         <!-- remediation: CSP's Planned Actions and Milestones -->

         <risk-status>open</risk-status>
         <remediation-tracking>
            <tracking-entry uuid="1b500d56-1936-41eb-8b60-a2984937ab89">
               <date-time-stamp>2020-07-02T00:00:00Z</date-time-stamp>
               <title>Activity 1</title>
               <description />
            </tracking-entry>
            <tracking-entry uuid="316fb3fe-927a-49a1-9a72-a58722862623">
               <date-time-stamp>2020-07-07T00:00:00Z</date-time-stamp>
               <title>Activity 2</title>
               <description />
            </tracking-entry>
            <tracking-entry uuid="0b09e341-cf3c-4de7-b728-751c6e88b653">
               <date-time-stamp>2020-07-07T00:00:00Z</date-time-stamp>
               <title>Closed</title>
               <description />
            </tracking-entry>
         </remediation-tracking>
      </risk>
   <!-- party -->
   </poam-item>
</poam-items>
```

Deviations and Vendor Dependency Requirements

FedRAMP's requirements for deviation requests and vendor dependency handling are defined in the Continuous Monitoring Strategy Guide, and remain the same when delivering content in OSCAL format.

Vendor Dependency	Last Vendor Check-in Date	Vendor Dependent Product Name	Original Risk Rating	Adjusted Risk Rating	Risk Adjustmen	False Positive	Operational Requiremen	Deviation Rationale	Supporting Documents
Yes	8/5/2014	Example Firewall	High	Moderate	Yes	No	Pending	Risk Adjustment : The example firewall scanned is just preliminary Operational Requirement: The port is needed for service example.	Remediation Evidence : filename.doc Deviation Request : DR-123-Example-1.doc

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

4.5. Deviations and Vendor Dependencies

After risks are identified a deviation may be appropriate, or a vendor dependency may exist. As deviations are identified, the initial risk information is not modified. Additional content is added to identify these changes. In each case, an additional `observation` is added to the `finding` assembly, and additional `risk-metric` fields are added to the risk assembly. There may be both Operational Requirement (OR) and Risk Assessment (RA) information in the same `finding` assembly.

4.5.1. False Positive (FP)

To document a false positive add a `risk-metric` field, an `observation` assembly, and change the `risk-status` to "`closed`". Set the `risk-metric` field's `name` to "`false-positive`", the `system` to "`https://fedramp.gov`", and the value to "`pending`". Once approved by the authorizing official(s), change the value to "`approved`". If the OR is rejected, remove the `risk-metric` field.

Within the `observation` assembly, provide a description of the false positive. This must have a conformity tag with a value of "`false-positive`". Typically the `observation-method` is set to `EXAMINE`; however, another method may be identified if more appropriate.

Finally, add a separate `relevant-evidence` assembly for each piece of evidence supporting the FP. Attached evidence, such as screen shots, must be defined as a `resource` in the `back-matter`, and cited using a URI fragment (hashtag, followed by the UUID of the `resource`.)

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->
      <observation uuid="46209140-8263-4e74-b3c9-cead4ffed22c">
         <title>False Positive</title>
         <description><p>False positive justification.</p></description>
         <prop name="conformity"
                        ns="https://fedramp.gov/ns/oscal">false-positive</prop>
         <observation-method>EXAMINE</observation-method>

         <relevant-evidence href="#53af7193-b25d-4ed2-a82f-5954d2d0df61">
            <description>
               <p>A screen shot showing the setting is correct</p></description>
         </relevant-evidence>

         <relevant-evidence href="https://vendor.site/describing/something.htm">
            <description>
               <p>Vendor detail describing why this happens.</p></description>
         </relevant-evidence>
      </observation>

      <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
         <!-- title, description -->
         <!-- initial risk metrics -->
         <risk-metric name="false-positive"
                      system="https://fedramp.gov">pending</risk-metric>
         <!-- risk statement -->
         <risk-status>closed</risk-status>
      </risk>
   <!-- party -->
   </poam-item>
</poam-items>
```

Vendor Dependency	Last Vendor Check-in Date	Vendor Dependent Product Name	Original Risk Rating	Adjusted Risk Rating	Risk Adjustment	False Positive	Operational Requirement	Deviation Rationale	Supporting Documents
Yes	8/5/2014	Example Firewall	High	Moderate	Yes	No	Pending	Risk Adjustment : The example firewall scanned is just preliminary Operational Requirement: The port is needed for service example.	Remediation Evidence : filename.doc Deviation Request : DR-123-Example-1.doc

An operationally required risk is an open risk, which is allowed to remain.

The `risk-status` must remain "`open`". Do not set the `risk-status` to "`closed`".

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

4.5.2. Operationally Required (OR)

To document an operationally required risk, add a `risk-metric` field and an `observation` assembly. The `risk-status` remains set to "`open`". Set the `risk-metric` field's `name` to "`operational-requirement`", the `system` to "`https://fedramp.gov`", and the value to "`pending`". Once approved by the authorizing official(s), change the value to "`approved`". If the OR is rejected, remove the `risk-metric` field.

Within the `observation` assembly, provide a justification for the operational requirement. This must have a conformity tag with a value of "`operational-requirement`". Typically the `observation-method` is set to `EXAMINE`; however, another method may be identified if more appropriate.

Finally, add a separate `relevant-evidence` assembly for each piece of evidence supporting the OR. Attached evidence, such as screen shots, must be defined as a `resource` in the `back-matter`, and cited using a URI fragment (hashtag, followed by the UUID of the `resource`.)

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->

      <observation uuid="9de7cba9-40fc-4c4d-b6af-01bd24f1def6">
         <title>Operational Requirement</title>
         <description><p>Justification for the OR.</p></description>
         <prop name="conformity"
               ns="https://fedramp.gov/ns/oscal">operational-requirement</prop>
         <observation-method>EXAMINE</observation-method>

         <relevant-evidence href="#53af7193-b25d-4ed2-a82f-5954d2d0df61">
            <description>
               <p>Screen shot showing impact when patched.</p>
            </description>
         </relevant-evidence>

         <relevant-evidence
                     href="https://vendor.site/article/describing/something.htm">
            <description>
               <p>Vendor detail describing why this happens.</p>
            </description>
         </relevant-evidence>
      </observation>

      <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
         <!-- title, description -->

         <!-- initial risk metrics -->
         <risk-metric name="operational-requirement"
                      system="https://fedramp.gov">pending</risk-metric>

         <!-- risk statement -->
         <risk-status>open</risk-status>
      </risk>
   <!-- party -->
   </poam-item>
</poam-items>
```

Vendor Dependency	Last Vendor Check-in Date	Vendor Dependent Product Name	Original Risk Rating	Adjusted Risk Rating	Risk Adjustment	False Positive	Operational Requirement	Deviation Rationale	Supporting Documents
Yes	8/5/2014	Example Firewall	High	Moderate	Yes	No	Pending	Risk Adjustment : The example firewall scanned is just preliminary Operational Requirement: The port is needed for service example.	Remediation Evidence : filename.doc Deviation Request : DR-123-Example-1.doc

Calculated Risk

Both *initial* and *residual* risk values are calculated based on likelihood and impact values.

Every POA&M entry must have initial likelihood and impact values:

```
<risk-metric name="likelihood" class="initial"
                               system="https://fedramp.gov">high</risk-metric>
<risk-metric name="impact"     class="initial"
                               system="https://fedramp.gov">moderate</risk-metric>
```

When justifying a risk adjustment, either the likelihood or impact may be lowered. It is possible to justify lowering both. Even if just one value is lowered, both residual risk values must be present:

```
<risk-metric name="likelihood" class="residual"
                               system="https://fedramp.gov">moderate</risk-metric>
<risk-metric name="impact"     class="residual"
                               system="https://fedramp.gov">moderate</risk-metric>
```

Using the Common Vulnerability Scoring System (CVSS)

When using CVSS scoring to justify a risk adjustment, the CVSS metrics are added as additional risk-metric fields. There must be one risk-metric field for each CVSS metric.

```
<risk-metric name="AV" system="CVSSv3.1">network</risk-metric>
```

See *Appendix A, CVSS Scoring* for more information.

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

4.5.3. Risk Adjustment (RA)

To document a risk adjustment, add `risk-metric` fields, `mitigating-factor` assemblies, and an `observation` assembly. The `risk-status` remains set to "`open`". Set the `risk-metric` field's `name` to "`risk-adjustment`", the `system` to "`https://fedramp.gov`", and the value to "`pending`". Once approved by the authorizing official(s), change the value to "`approved`". If the OR is rejected, remove the `risk-metric` field.

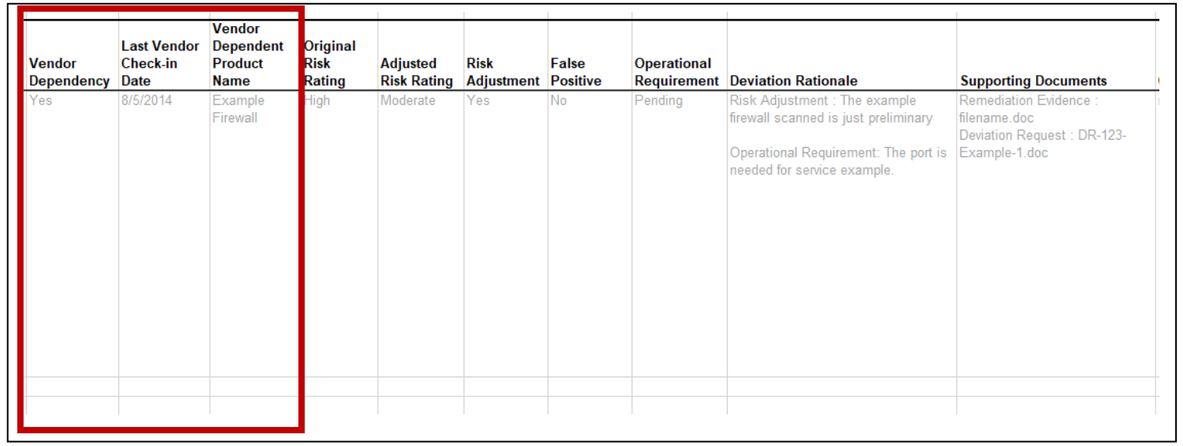
Within the `observation` assembly, provide a justification for the risk adjustment. This must have a conformity tag with a value of "`risk-adjustment`". Typically the `observation-method` is set to `EXAMINE`; however, another method may be identified if more appropriate.

Provide an additional `risk-metric` field with the `name` set to "`risk-adjustment`". Risk is adjusted by lowering either likelihood, impact, or both. Add additional `risk-metric` fields with the `class` set to "`residual`" and the adjusted value. All risk-metric fields described here must have the `system` set to "`https://fedramp.gov`".

Finally, include one or more `mitigating-factor` assemblies. One describing each mitigating factor. If an SSP implementation statement describes the mitigating factor, link to it using the `implementation-uuid` flag.

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->

      <observation uuid="7acee179-1570-4ea0-94dc-01b8c0a29c0a">
         <title>Risk Adjustment</title>
         <description><p>Justify the risk.</p></description>
         <prop name="conformity"
                        ns="https://fedramp.gov/ns/oscal">risk-adjustment</prop>
         <observation-method>EXAMINE</observation-method>
      </observation>

      <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
         <!-- title, description -->
         <!-- initial risk metrics -->

         <risk-metric name="risk-adjustment"
                      system="https://fedramp.gov">assessor-validated</risk-metric>
         <risk-metric name="impact"     class="residual"
                                system="https://fedramp.gov">high</risk-metric>
         <risk-metric name="likelihood" class="residual"
                                system="https://fedramp.gov">high</risk-metric>


         <mitigating-factor uuid="260d3c0a-fc2e-4627-9fb9-a003acdc4b14">
            <description><p>Describe mitigating factor</p></description>
         </mitigating-factor>

         <mitigating-factor uuid="fd061039-e9b0-4b4c-a78b-ca024d411174"
                      implementation-uuid="46f4c261-e488-4fb5-84d6-6a61dd30c3d7">
            <description><p>How cited impl. statement lowers risk.</p></description>
         </mitigating-factor>

         <!-- risk statement, risk status -->
      </risk>
   </poam-item>
</poam-items>
```



Vendor Dependency	Last Vendor Check-in Date	Vendor Dependent Product Name	Original Risk Rating	Adjusted Risk Rating	Risk Adjustment	False Positive	Operational Requirement	Deviation Rationale	Supporting Documents
Yes	8/5/2014	Example Firewall	High	Moderate	Yes	No	Pending	Risk Adjustment : The example firewall scanned is just preliminary Operational Requirement: The port is needed for service example.	Remediation Evidence : filename.doc Deviation Request : DR-123-Example-1.doc

If the Vendor Dependent Product Name is not already defined as an individual component, add a `component` to the `local-definitions` assembly describing the component.

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

4.5.4. Vendor Dependency

To document a vendor dependency, add a `risk-metric` field and an `observation` assembly. The `risk-status` remains set to "`open`". Set the `risk-metric` field's `name` to "`vendor-dependency`", the `system` to "`https://fedramp.gov`" , and the value to "`tracking`". Once the vendor has resolved the dependency, change the value to "`resolved`".

Within the `observation` assembly, explain the dependency in the `description` field. This must have a conformity tag with a value of "`vendor-dependency`". Typically the `observation-method` is set to `INTERVIEW`; however, another method may be identified if more appropriate.

The `observation` assembly must include a `subject-reference` identifying the component. The Vendor Dependency Product Name is provided from the component details. If an appropriate component is not defined, create one within the `local-definitions` assembly.

Add a separate `relevant-evidence` assembly for each piece of evidence supporting the dependency. Attached evidence, such as screen shots, must be defined as a `resource` in the `back-matter`, and cited using a URI fragment (hashtag, followed by the UUID of the `resource`.)

As the CSP performs the required regular vendor check-ins, each must be added to the `remediation-tracking` assembly as an additional `tracking-entry`. The `title` should be set to "`Vendor Check-in`", the `date-time-stamp` must indicate when the check-in occurred. The result of the check-in must be described in the `description` field. Each vendor check-in entry must have a `conformity` tag with the value set to "`vendor-check-in`".

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->

      <observation uuid="6c103050-d72a-4391-b830-dc669641231c">
         <title>Vendor Dependency</title>
         <description><p>Describe the vendor dependency here.</p></description>
         <prop name="conformity"
                        ns="https://fedramp.gov/ns/oscal">vendor-dependency</prop>
         <observation-method>INTERVIEW</observation-method>
         <subject-reference uuid-ref="uuid-cut" type="component" />
      </observation>

      <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
         <!-- title, description, risk-metric, risk-metric -->
         <risk-metric name="vendor-dependency"
                                    system="https://fedramp.gov">tracking</risk-metric>

         <!-- risk statement, risk status -->
         <remediation-tracking>
            <!-- tracking-entry -->
            <tracking-entry uuid="d084a039-bdd1-4ccd-a06a-53355e07fa2f">
               <date-time-stamp>2020-07-07T00:00:00Z</date-time-stamp>
               <title>Vendor Check-in</title>
               <description><p>Description result of the check-in.</p></description>
               <prop name='conformity'
                           ns='https://fedramp.gov/ns/oscal'>vendor-check-in</prop>
            </tracking-entry>
         </remediation-tracking>         </risk>
   </poam-item>
</poam-items>
```

[Image intentionally left blank.]

4.5.5. Evidence and Artifacts

All evidence collected must be attached (by relative URI path 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`".

Additional type fields may also be added 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`.

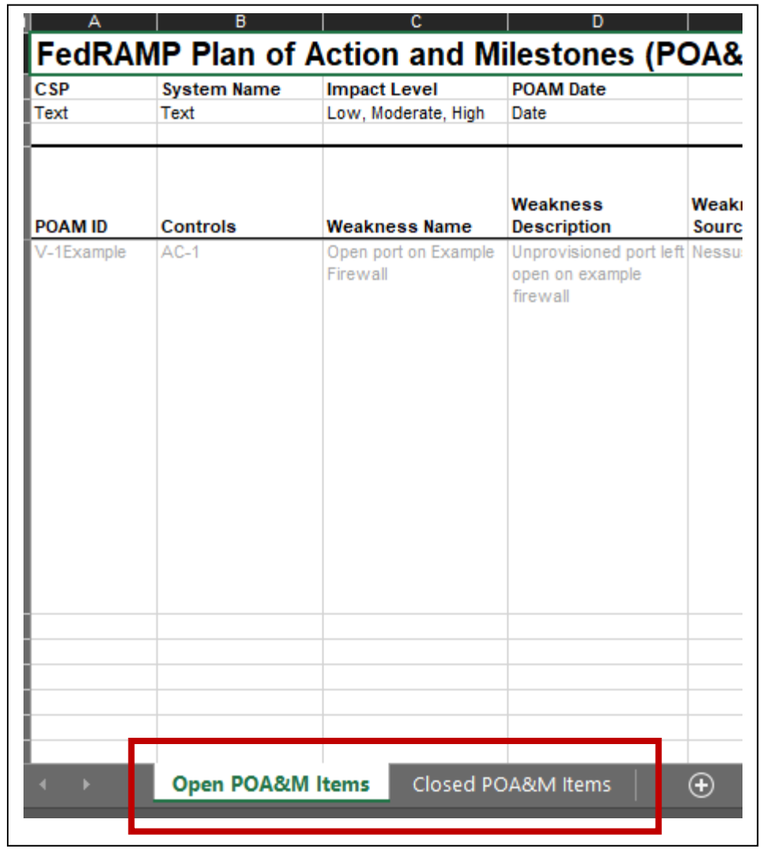
Evidence may be cited from an `observation` as `relative-evidence`.

A POA&M 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 within the same `resource` assembly. This may be useful if the CSP 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

```
<!-- poam-items -->
<back-matter>
   <resource uuid="f32b7ab1-baf1-451a-b3a1-1dfdadbe8dc7">
      <title>[EXAMPLE]AC Policy</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">evidence</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>
```



The `description` and `closure-actions` 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

4.6. Risk Closure

Once identified, risks must remain in the POA&M. To represent a risk closure, change the `risk-status` to "`closed`", then add a `closure-action` field and a final `tracking-entry` assembly to the `remediation-tracking` assembly.

In the `closure-action` field, describe the action(s) taken by the CSP to close the risk.

In the `remediation-tracking` assembly there must be at least one `tracking-entry` assembly with the `date-time-stamp` field set to the date of closure and a `title` field set to "`Closed`". The `description` field must be present, but may be blank. Additional `tracking-entry` fields may be present; however, there should typically not be any entry with a `date-time-stamp` value later than the "`Closed`" `date-time-stamp` value.

If it is appropriate to attach evidence of closure, add an `observation` assembly with the appropriate evidence attached. If used, the `observation` assembly must have a `conformity` tag of "`risk-closure`".

Representation

```
<poam-items uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <poam-item uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <!-- title, description, date-time-stamp, observation(s) -->

      <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
         <!-- title, description, risk metrics, risk-statement -->

         <!-- remediation: tool recommendation -->
         <!-- remediation: CSP's plan and schedule -->

         <risk-status>closed</risk-status>
         <closure-actions>
            <p>Describe what action(s) the CSP took to close the risk.</p>
            <p>This field is only present when the risk-status is "closed".</p>
            <p>If the risk-status field is set to "open" this field is ignored.</p>
         </closure-actions>
         <remediation-tracking>
            <!-- tracking-entry: action taken -->
            <!-- tracking-entry: action taken -->
            <!-- tracking-entry: action taken -->
            <tracking-entry uuid="0b09e341-cf3c-4de7-b728-751c6e88b653">
               <date-time-stamp>2020-07-07T00:00:00Z</date-time-stamp>
               <title>Closed</title>
               <description />
            </tracking-entry>
         </remediation-tracking>
      </risk>
   <!-- party -->
   </poam-item>
</poam-items>
```

APPENDICIES

APPENDIX A. CVSS SCORING

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

The FedRAMP OSCAL Registry includes a *Risk Metrics* tab with the specific `name` and `system` 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.

Tools should accept either the upper-case abbreviation or the lower-case name on a field-by-field basis. For example, it should be acceptable to use "`AV`" for access vector, and "`privileges-required`" for privileges required, provided both have a class value of "CVSSv3.1".

All CVSS metrics must be in the same CVSS version, as identified by the `system` flag, for successful computation. Tool developers should ensure the tool performs CVSS calculations as defined by the Forum of Incident Response and Security Teams (FIRST) at https://www.first.org/cvss/.

Representation

```
<poam-items id="77638952-cb0a-44e5-ac31-f0d0d29f1bb1">
   <!-- title, description, start, end -->
   <poam-item 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, description -->

         <!-- CVSS Metrics using V3.1 using abbreviations -->
         <risk-metric name="AV" system="CVSSv3.1">network</prop>

         <risk-metric name="AC" system="CVSSv3.1">high</prop>

         <risk-metric name="PR" system="CVSSv3.1">low</prop>

         <!-- CVSS Metrics using V3.1 using names -->
         <risk-metric name="access-vector"
                                        system="CVSSv3.1">network</prop>

         <risk-metric name="access-complexity"
                                        system="CVSSv3.1">high</prop>

         <risk-metric name="privileges-required"
                                        system="CVSSv3.1">low</prop>

         <!-- risk-statement, risk-status -->
      </risk>
   </poam-item>
</poam-items>
```