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

fedramp1.1.0-oscal1.0.0

August 12, 2021

FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
8/1/2020	Initial Publication	1.0	FedRAMP PMO
2/25/2021	Revised to align with OSCAL RC-2 Syntax	2.0	FedRAMP PMO
4/30/2021	Finalize alignment with OSCAL RC-2 Syntax.	2.1	FedRAMP PMO
7/6/2021	Finalize alignment with OSCAL 1.0.0 Syntax	fedramp1.0.0-oscal1.0.0	FedRAMP PMO
7/28/2021	Hyperlink updates and various errata fixes.	fedramp1.0.1-oscal1.0.0	FedRAMP PMO
8/11/2021	Review for updated release.	fedramp1.0.2-oscal1.0.0	FedRAMP PMO
8/12/2021	Review for updated release.	fedramp1.1.0-oscal1.0.0	FedRAMP PMO

How to Contact Us

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

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

TABLE OF CONTENTS

Document Revision History i

1. Overview 1

1.1. Who Should Use This Document? 1
1.2. Related Documents 1
1.3. Basic Terminology 2

2. FedRAMP Extensions and Allowed Values 3

3. Working with OSCAL Files 4

3.1. XML and JSON Formats 4
3.2. POA&M File Concepts 4
3.2.1. Resolved Profile Catalogs 6
3.3. OSCAL-based FedRAMP POA&M Template 7
3.4. OSCAL's Minimum File Requirements 8
3.5. Importing the System Security Plan 9
3.5.1. When OSCAL-based SSP Information is Inaccurate 10
3.5.2. Delivering the POA&M and Inventory Without the SSP 11

4. POA&M Template to OSCAL Mapping 12

4.1. Representing the POA&M 12
4.2. Individual POA&M Entries 13
4.2.1. Individual POA&M Entries: Findings 14
4.2.2. Individual POA&M Entries: Observations 15
4.2.3. Individual POA&M Entries: Asset Identifiers 16
4.2.4. Individual POA&M Entries: Weakness Information 17
4.3. Recommended and Planned Remediation 18
4.3.1. Planned Remediation Schedule 19
4.4. Risk Tracking 20
4.5. Deviations and Vendor Dependencies 21
4.5.1. False Positive (FP) 21
4.5.2. Operationally Required (OR) 22
4.5.3. Risk Adjustment (RA) 23
4.5.4. Vendor Dependency 24
4.5.5. Evidence and Artifacts 25
4.6. Risk Closure 26

Appendix A. CVSS Scoring 27

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 AND ALLOWED 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.

A summary of the FedRAMP extensions and allowed values appears in the FedRAMP OSCAL Registry.

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

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 and allowed values. The extensions related to the Security Assessment Plan (SAP) are cited in this document in context of their use.

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

FedRAMP extensions and allowed values are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

Revised FedRAMP Registry Approach

The FedRAMP OSCAL Registry was originally provided as a spreadsheet. It now uses the draft OSCAL Extensions syntax and is offered in XML and JSON formats, with a human-readable HTML representation. This enables tools to be extension-aware.

- *XML Version*
- *JSON Version*
- *HTML Version*

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.

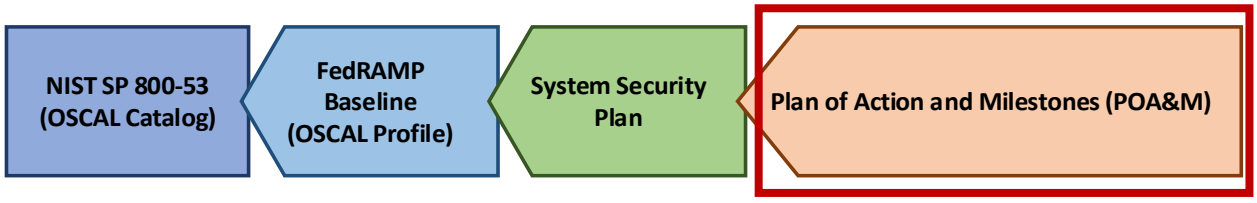
3.1. XML and JSON Formats

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.

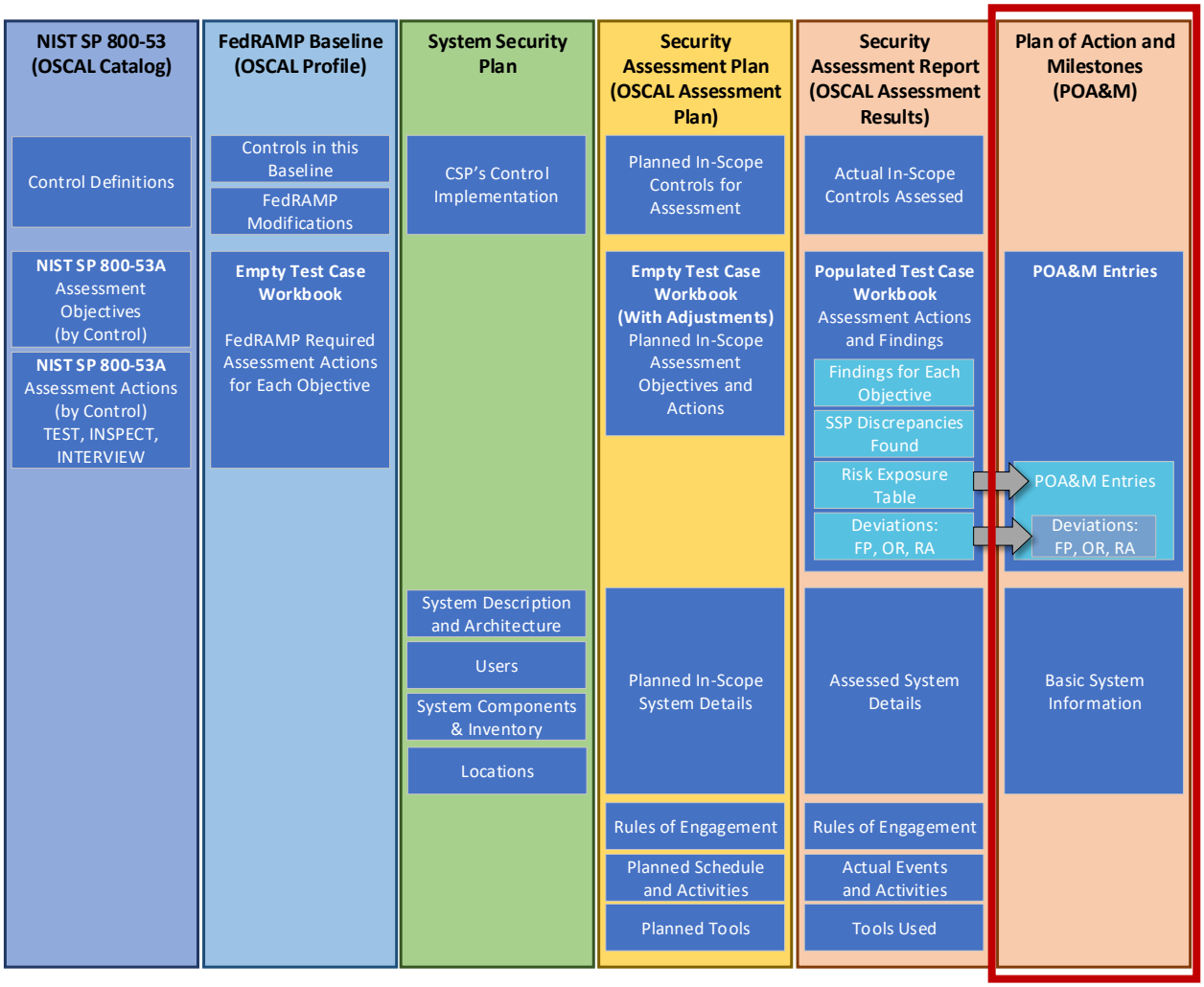
3.2. POA&M File Concepts

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.

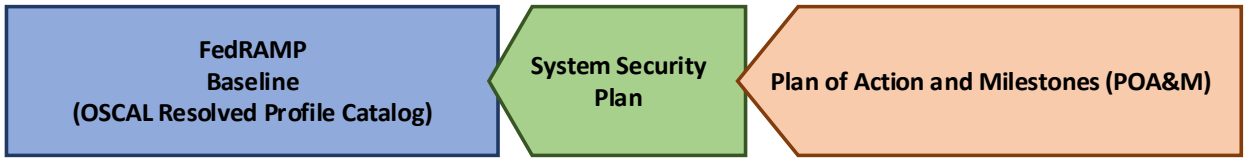
The POA&M also inherits the SSP's pointer to the appropriate OSCAL-based FedRAMP Baseline. Through that linkage, the POA&M references the control baseline definitions for the system's baseline.

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*.

3.3. OSCAL-based FedRAMP POA&M Template

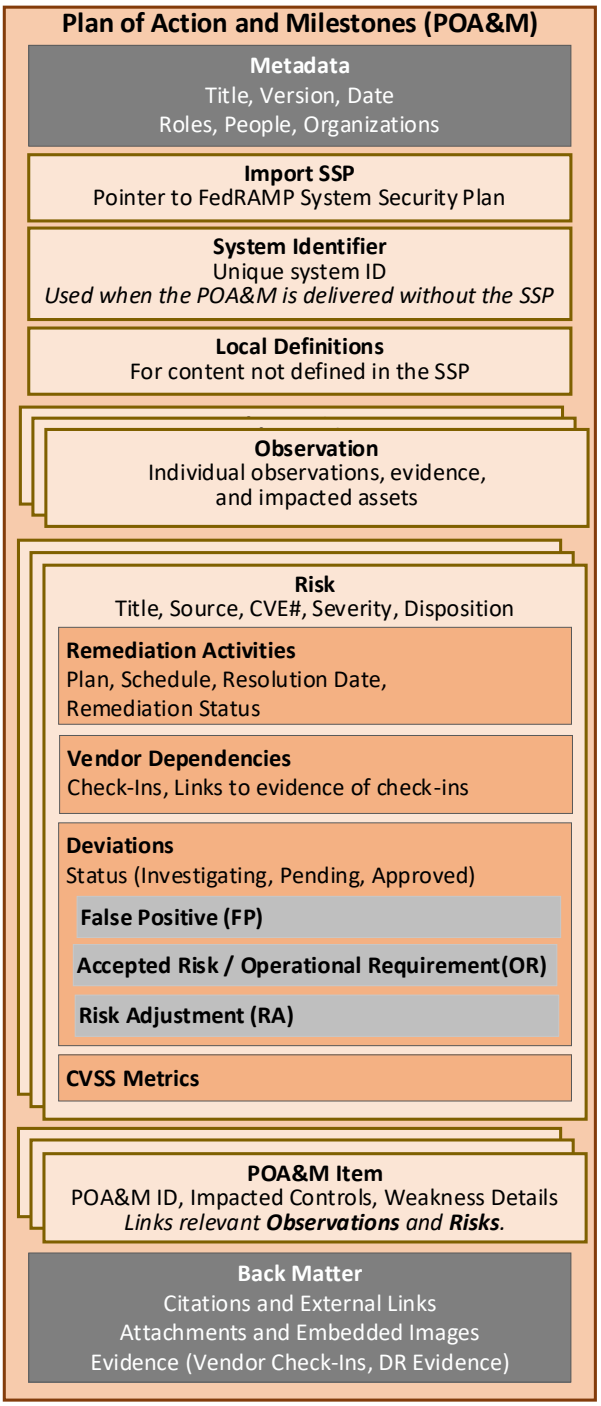
FedRAMP offers an OSCAL-based POA&M shell file in both XML and JSON formats. This shell contains many of the FedRAMP required standards to help get you started. This document is intended to work in concert with that file. The OSCAL-based FedRAMP POA&M Template is available in XML and JSON formats here:

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



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 monthly ConMon delivery of the POA&M without the SSP, 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-valueof-resource]" />
```

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 POA&M file's `back-matter`. Refer to the *Guide to OSCAL-based FedRAMP Content*, *Section 2.7, Citations and Attachments 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" value="ssp"/>
      <!-- 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. When OSCAL-based SSP Information is Inaccurate

Ideally, when SSP information is missing or inaccurate the system ISSO should correct the SSP.

If the POA&M must be updated with missing or inaccurate SSP information, the POA&M syntax allows for SSP information correction.

Tool designers should ensure their tools can cite the relevant OSCAL-based SSP information when possible, and capture assessor-corrected SSP information in the POA&M's `local-definitions` or `metadata` sections when necessary. The relevant sections of this guide describe how to represent inaccurate SSP information in the POA&M when needed.

Monthly Continuous Monitoring (ConMon) Delivery

For monthly ConMon deliveries, the CSP may duplicate the component and inventory-item content from their SSP into the POA&M's local-definitions section. Delivering an OSCAL POA&M with all inventory in this way satisfies both the POA&M and System Inventory deliverables.

3.5.2. Delivering the POA&M and Inventory Without the SSP

FedRAMP currently requires CSPs to deliver their POA&M, system inventory, and raw scanner tool output each month. OSCAL enables the delivery of POA&M and inventory without delivering the linked SSP.

In this instance, the OSCAL allows the `import-ssp` syntax to be omitted; however, FedRAMP still requires the `system-id` content containing the system's FedRAMP-assigned unique identifier.

All SSP `inventory-item` assemblies must be duplicated into the POA&M `local-definitions` assembly. Any SSP `component` cited by an `inventory-item` must also be duplicated to the POA&M's local-definitions assembly. Finally, any SSP `component` referenced by POA&M data must be duplicated, whether it is referenced by an inventory-item or not.

SAP Representation

```
<system-id identifier-type="https://fedramp.gov">F00000000</system-id>

<local-definitions>

   <component uuid="uuid-value" type="software">
      <!-- cut -->
   </component>
   <component uuid="uuid-value" type="software">
      <!-- cut -->
   </component>

   <inventory-item uuid="uuid-value">
      <!-- cut -->
   </inventory-item>
   <inventory-item uuid="uuid-value">
      <!-- cut -->
   </inventory-item>


   <inventory-item uuid="uuid-value">
      <!-- cut -->
      <implemented-component component-uuid="uuid-of-component" />
   </inventory-item>
   <inventory-item uuid="uuid-value">
      <!-- cut -->
      <implemented-component component-uuid="uuid-of-component" />
   </inventory-item>
</local-definitions>
```

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
- Observations
- Risks; 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 that guide, this document refers to them and only adds details that are unique to the POA&M.

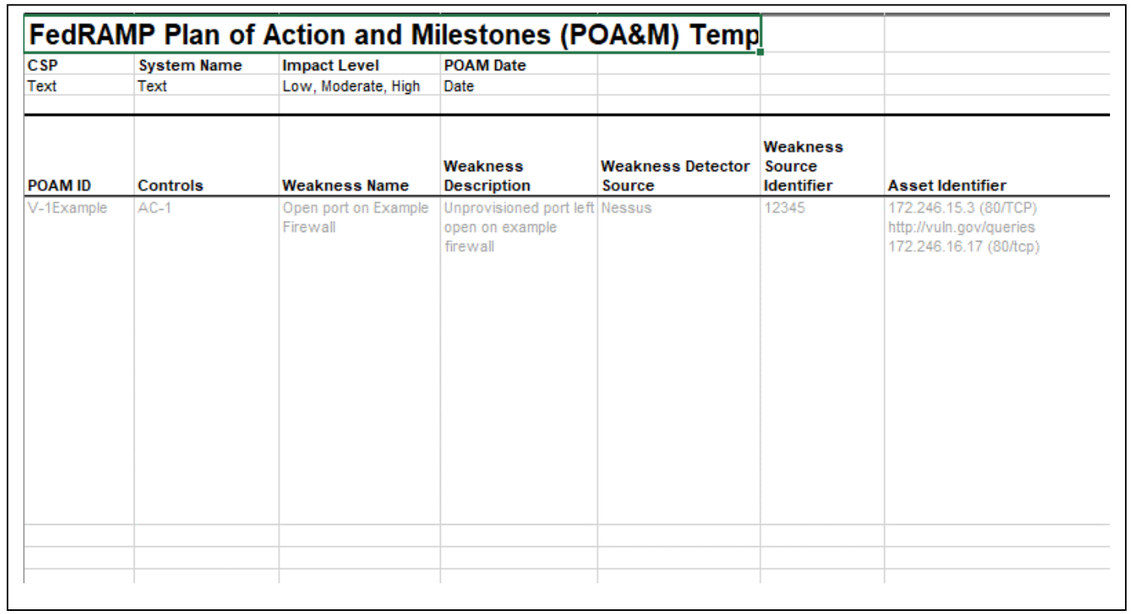
4.1. Representing the POA&M

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

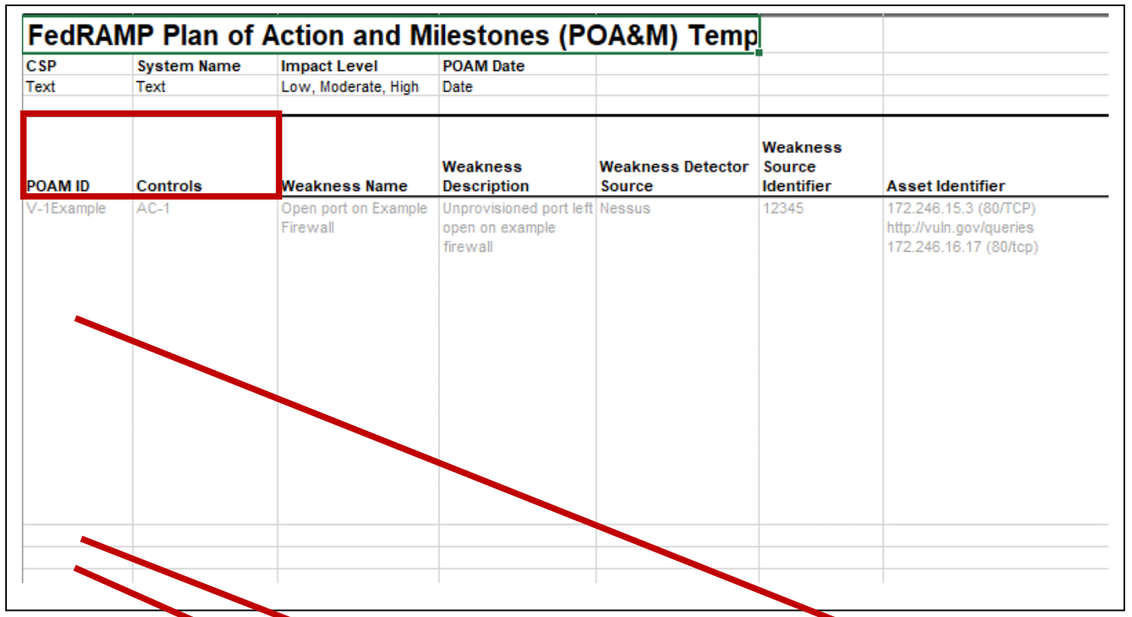
4.2. Individual POA&M Entries

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 in OSCAL.

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.

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 -->
   <!-- observation 1 -->
   <!-- observation 2 -->
   <!-- observation 3 -->
   <!-- risk A -->
   <!-- risk A -->
   <!-- risk A -->

   <poam-item uuid="6F5FFF73-CAC6-4DA0-A0D9-0F931A5EFAFA">
      <title>[EXAMPLE]POA&amp;amp;M Item</title>
      <description/>
      <prop name="POAM-ID" ns=https://fedramp.gov/ns/oscal value="V-1"/>
      <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
      <associated-risk risk-uuid="9cbd98f3-abcb-4948-ad06-14e0bcba742f" />
      <remarks>
         <p>The FedRAMP Extension, "POAM-ID" captures the traditional CSP-assigned
unique POA&amp;amp;M identifier.</p>
         <p>The date-time-stamp identifies the date of discovery. FedRAMP is concerned
with the date information. The time information is desirable and should be included
where available. The time may be all zeros if unavailable.</p>
      </remarks>
   </poam-item>

   <!-- poam-item (spreadsheet row 2) -->
   <!-- poam-item(spreadsheet row 3) -->
   <!-- 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; however, in OSCAL, some of the details are included in `observation` or `risk` assemblies and linked to the `poam-item` assembly.

The `observation` assembly identifies who, what, where, when and how. It identifies who performed what activity, how the activity was performed, what tools were used, and what evidence was collected. If appropriate, the location can be included as well. **More importantly, `observation` identifies the system components impacted by the risk.**

The `risk` assembly includes risk details, such as the risk statement, likelihood, impact, mitigating factors, deviations, remediation plan, and resolution tracking. OSCAL allows more than one `associated-risk` to be assigned to be assigned to a `poam-item`; however, FedRAMP strongly recommends only one `associated-risk` per `poam-item`.

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

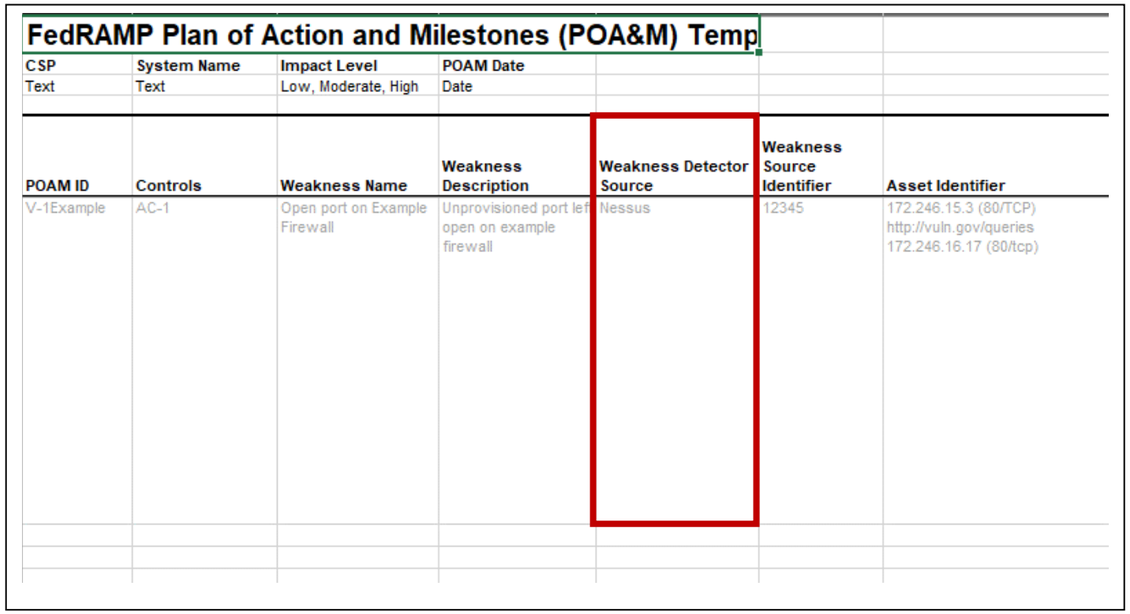
The related control must be present in the `risk` assembly using the "impacted-control-id" FedRAMP extension.

The `collected` field must be set to the Original Detection Date, which may be the tool's timestamp.

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

Representation

```
   <observation uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab">
      <!-- evidence details: which tool, who operated it, where is the raw output? -->
   </observation>
   <!-- observation -->
   <!-- observation -->

   <risk uuid="9cbd98f3-abcb-4948-ad06-14e0bcba742f">
      <prop name="impacted-control-id" ns="https://fedramp.gov/ns/oscal" value="ac-2" />
      <!-- risk details: likelihood, impact, mitigation, deviation, remediation -->
   </risk>
   <!-- risk -->
   <!-- risk -->

   <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" value="V-1"/>
       <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
       <associated-risk risk-uuid="9cbd98f3-abcb-4948-ad06-14e0bcba742f" />

   </poam-item>

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

   <!-- poam-item -->
      <!-- related-observation -->
      <!-- associated-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 `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 `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`".

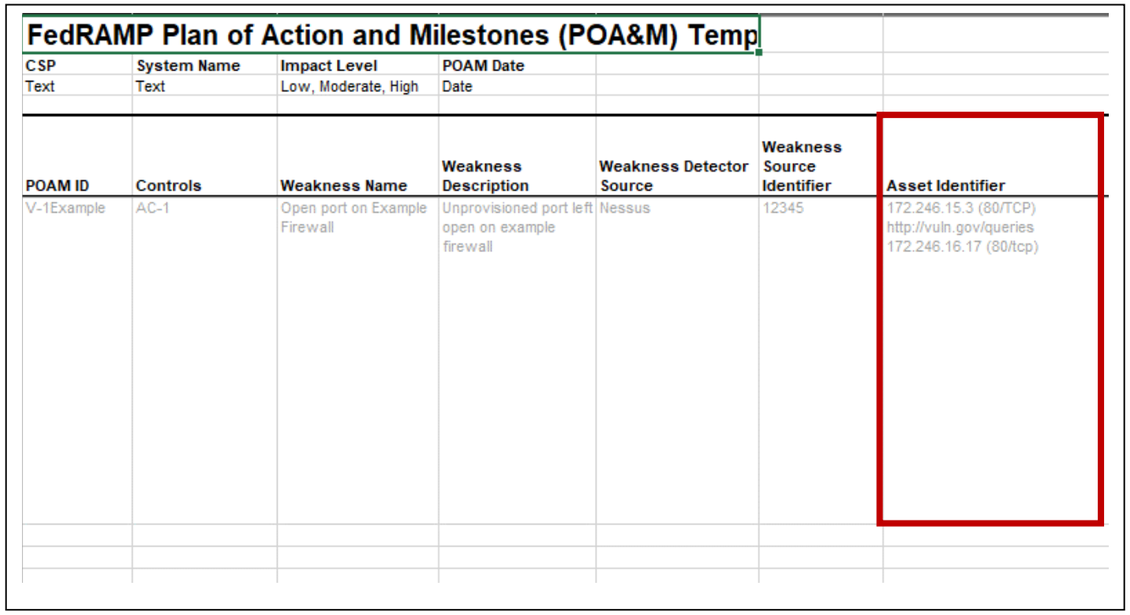
> The tool must be defined as a `component` in the `local-definitions` assembly, using the same syntax and approach described in the *Guide to OSCAL-based Security Assessment Plans (SAP)*, *Section 4.14, SAP Test Plan: Testing Performed Using Automated Tools*. If the POA&M item was identified another 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 `finding` 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" type="software">
         <title>XYZ Vulnerability Scanning Tool</title>
         <description/>
         <prop name="vendor" value="Vendor Name"/>
         <prop name="name" value="Tool Name"/>
         <prop name="version" value="1.2.3"/>
         <status state="operational"/>
      </component>
</local-definitions>

<observation uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab">
   <description><p></p></description>
   <method>TEST</method>
   <origin>
      <actor type="party" uuid-ref="f4568fda-c6d2-4640-adec-0012015af7d0" />
      <actor type="tool"  uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
   </origin>
   <relevant-evidence href="./raw_scans/scanner_output.csv">
      <description><p>Optional pointer to the raw scanner output that generated
                                                this POA&amp;M entry.</p></description>
   </relevant-evidence>
   <collected>2020-10-10T00:00:00Z</collected>
</observation>

<!-- risk -->

<poam-item uuid="0be71cd3-f850-47db-836f-14511edbd90e">
   <!-- cut -->
    <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
</poam-item>
```



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 0, FedRAMP currently* requires CSPs to deliver their POA&M, system inventory, and raw scanner tool output each month. OSCAL enables the delivery of POA&M and inventory without delivering the linked SSP.

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

SAP Representation

```
<system-id identifier-type="https://fedramp.gov">F00000000</system-id>

<local-definitions>

   <component uuid="uuid-value" type="software">
      <!-- cut -->
   </component>
   <component uuid="uuid-value" type="software">
      <!-- cut -->
```

4.2.3. Individual POA&M Entries: Asset Identifiers

For scanner tool findings, impacted assets are identified using the `subject` 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.

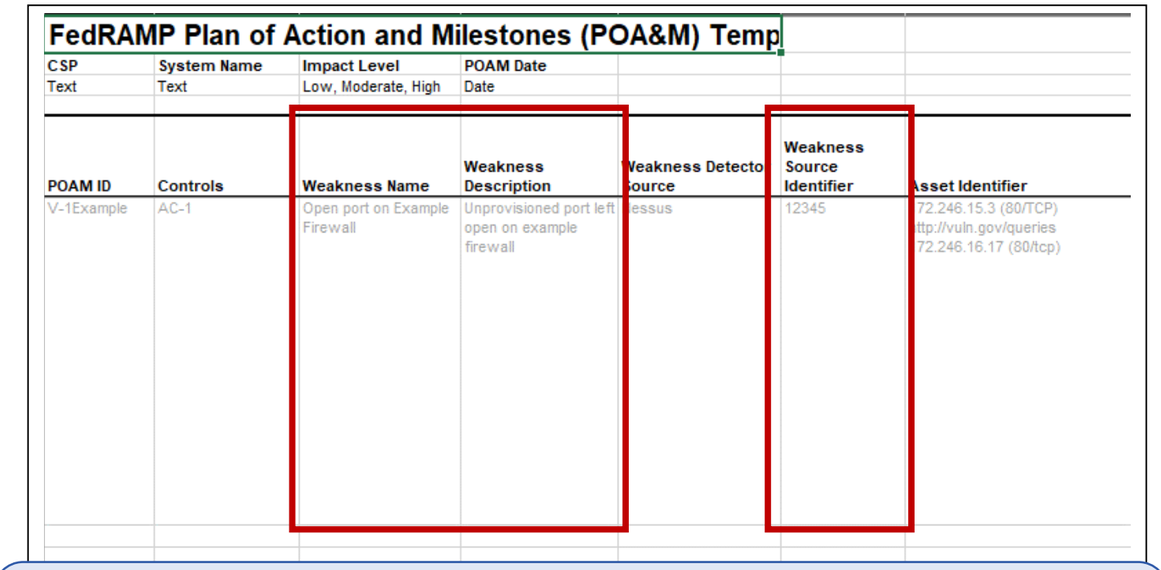
All details about the asset become available as a result of that UUID reference, such as IP address, fully qualified domain name (FQDN), and the asset's point of contact. If an inventory-item contains an `implemented-component` field, those linked component details are also considered to be part of the inventory-item itself.

When providing a monthly POA&M to FedRAMP using OSCAL, the 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.

Representation

```
   <local-definitions>
      <component uuid="75b059f2-a9ba-40b1-a1e0-881196ca1ead" 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">
         <description><p>An instance of the above component.</p></description>
         <prop name="ipv4-address" value="10.10.10.10"/>
         <prop name="fqdn" value="host.domain.cloud"/>
         <implemented-component component-id="a49ed61e-fca1-4ffa-b5e7-c23a2375a7a0"
                                                              use="runs-software" />
      </inventory-item>
      <inventory-item uuid="02075556-3660-4112-8982-02fc7d6fac00" />   <!-- cut -->
      <inventory-item uuid="5efe2c07-9fdf-453a-8457-6471046082fb" />   <!-- cut -->
   </local-definitions>

   <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
      <!-- description, method, type -->
      <subject type="component" uuid-ref="75b059f2-a9ba-40b1-a1e0-881196ca1ead" />
      <subject type="inventory-item" uuid-ref="f61f4408-2cb8-444a-a312-bc88412e7c61" />
      <subject type="inventory-item" uuid-ref="02075556-3660-4112-8982-02fc7d6fac00" />
      <subject type="inventory-item" uuid-ref="5efe2c07-9fdf-453a-8457-6471046082fb" />
      <!-- origin, relevant-evidence -->
   </observation>
   <!-- risk -->
   <poam-item uuid="0be71cd3-f850-47db-836f-14511edbd90e">
      <!-- title, description, POA&M ID, collected -->
       <related-observation observation-uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d" />
   </poam-item>
```



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 `facet` 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. If the system is subject to multiple frameworks using different risk score values or risk calculation methods, they may each be expressed in their own `characterization` assembly.

Common values for the `system` flag include:

- `FedRAMP: https://fedramp.gov`
- `USCERT IAVM: https://us-cert.cisa.gov`
- `CVE: http://cve.mitre.org`
- `CVSS: (v2): http://www.first.org/cvss/v2,`
  `(v3): http://www.first.org/cvss/v3,`
  `(v3.1): http://www.first.org/cvss/v3.1`

If a tool provides a value with no clearly source of information for defining the value, use the special "unknown" system value: `http://csrc.nist.gov/ns/oscal/unknown`

Ideally scanner tool vendors will define a "system" value for their own tools. Until that happens, FedRAMP recommends either using the URL for the vendor's web site or the NIST-defined system value for an "unknown system: `http://csrc.nist.gov/ns/oscal/unknown`

Until this matures and clear system values are widely available across the industry, FedRAMP only requires the same system value be used consistently throughout the POA&M for a given tool, and keep the facet values from a given tool within the same characterization assembly which cites the tool as an actor.

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 `status` field is initially set to "open".

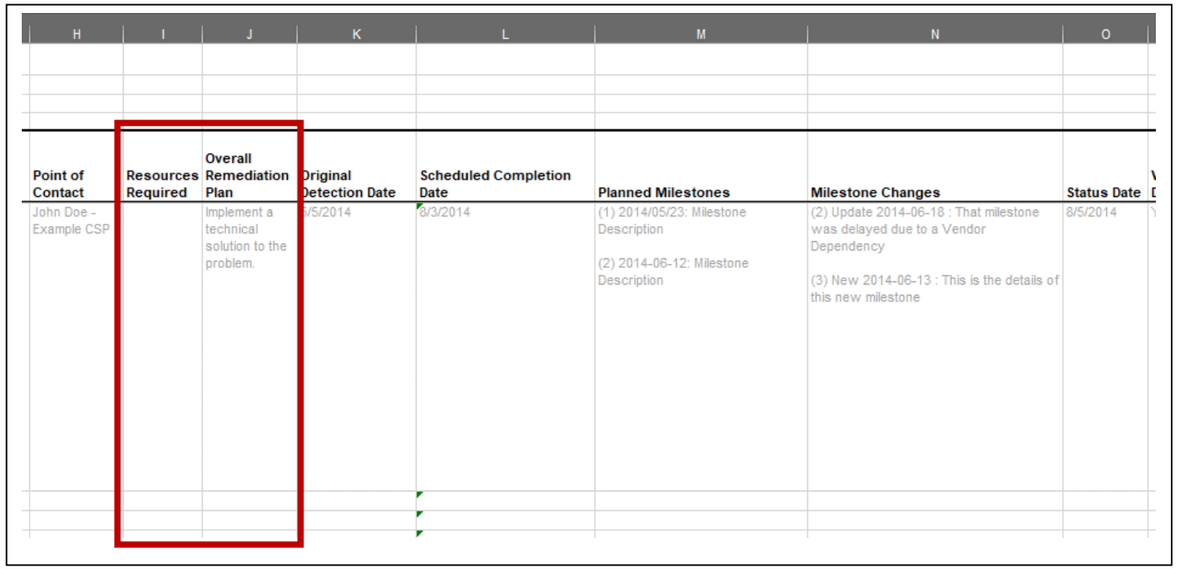
The Weakness Source Identifier requires a FedRAMP extension. Within the characterization's origin, an `actor` must be specified for the tool itself. Assign the "vulnerability-id" and "plugin-id" FedRAMP extensions as properties to this `actor`.

And information provided by the tool that characterizes the risk are captured as `facet` fields. When the scanner tool provides risk values from other recognized systems, such as a CVE number, IAVAM severity, or CVSS metric, the NIST-defined `name` and `system` values must be used, in addition to the tool value being assigned to the `value` attribute. For example, if the scanner tool provides a CVE number, the `risk-metric` field's `system` flag should reflect "`http://cve.mitre.org`" as the system, not the scanner tool.

FedRAMP required `facet` fields, such as likelihood and impact, have a `system` flag with a value of "`https://fedramp.gov`". FedRAMP required facets must also have an `annotation` with the name flag set to "state" and the value flag set to either "`initial`" or "`adjusted`". There must always be "initial" facets. If adjusted, there may be a "adjusted" facets as well.

Representation

```
<risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
   <title>Weakness Name</title>
   <description><p>This is the Weakness Description.</p></description>

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

   <characterization>
      <origin>
         <actor type="tool" actor-uuid="9d194268-a9d1-4c38-839f-9c4aa57bf71e">
            <prop name="vulnerability-id"
                                 ns="https://fedramp.gov/ns/oscal" value="VulID-001"/>
            <prop name="plugin-id"
                                 ns=https://fedramp.gov/ns/oscal value="Plugin-ID"/>
         </actor>
      </origin>
      <facet name="iavam-severity" value="high" system="https://us-cert.cisa.gov" />
      <facet name="AV" value="network"  system="http://www.first.org/cvss/v3.1" />
      <facet name="vulnerability-id" value="CVE-2020-00000"
                                       system="http://cve.mitre.org" />
      <facet name="impact" value="high"
                                       system="http://csrc.nist.gov/ns/oscal/unknown" />
   </characterization>
   <characterization>
      <origin>
         <actor type="party" uuid-ref="41E10E3B-32E1-4550-AE52-7F5D6B1BA532" />
      </origin>
      <facet name="likelihood" value="high" system="https://fedramp.gov">
         <annotation name="state" value="initial" />
      </facet>
      <facet name="impact" value="high" system="https://fedramp.gov">
         <annotation name="state" value="initial" />
      </facet>
      <facet name="priority" value="1" system="https://fedramp.gov" />
</risk>
```



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

4.3. Recommended and Planned Remediation

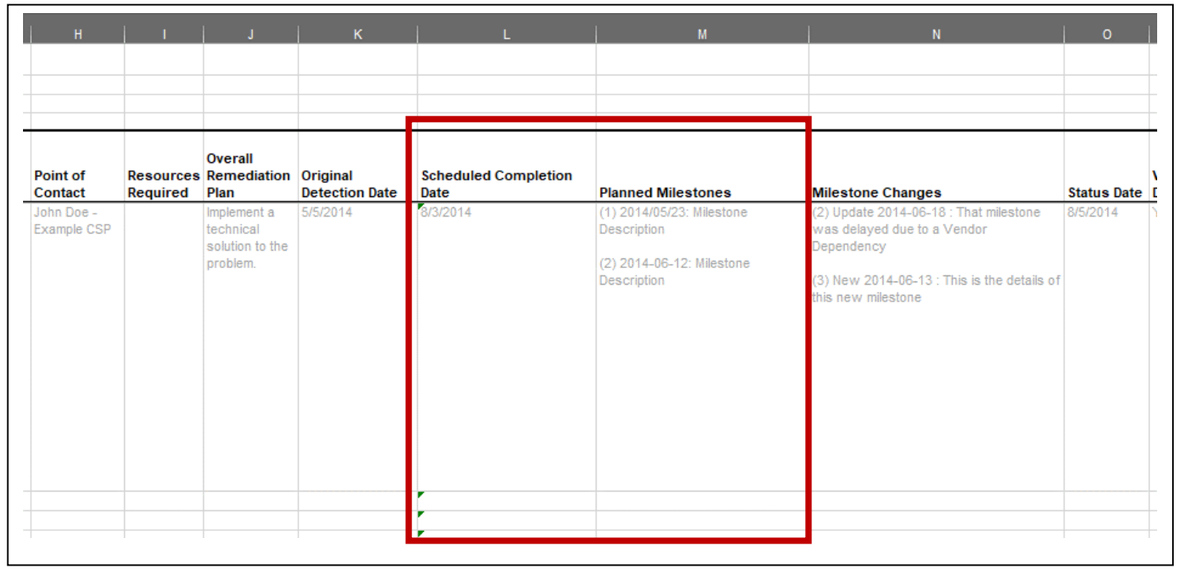
Within the `risk` assembly, there must be a `response` assembly containing the tool's recommended mitigation. The `type` flag must be set to "`recommendation`". The `origin` field's actor type flag must be set to "`tool`", and the `uuid-ref` must contain the UUID of the tool that generated the recommendation. Additional remediation recommendations may also be present, such as the assessor's recommendation copied from the SAR.

There must also be a `response` assembly containing the CSP's intended mitigation plan. The `type` flag must be set to "`planned`". The `origin` field's actor 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 the "planned" `response` assembly using the `required` assembly. Use the `description` field for a free-form explanation of required resources. Use one or more `subject` fields to link to a specific party, component, inventory-item, system user, or resource.

Representation

```
   <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
     <!-- title, description, statement, status, characterization -->
      <response uuid="a3106e23-8b79-4b1b-abf4-74f16c51ad0c" lifecycle="recommendation">
         <title>Tool's Recommendation</title>
         <description><p>Tool-provided recommendation.</p></description>
         <origin >
            <actor type="tool" actor-uuid="9d194268-a9d1-4c38-839f-
9c4aa57bf71e"></actor>
         </origin>
      </response>

      <response uuid="69344d05-937e-40f4-9c3f-9aa8702ad99d" lifecycle="recommendation">
         <title>Assessor's Recommendation</title>
         <description><p>Assessor-provided recommendation.</p></description>
         <origin >
            <actor type="party" uuid-ref="49f73135-efab-4275-9a79-003656ad890a"></actor>
         </origin>
      </response>

      <response uuid="e9ee6fe2-856f-42c7-8c2e-ff6466d31010" lifecycle="planned">
         <title>CSP's Remediation Plan</title>
         <description>
            <p>Describe the CSP's intended approach to remediating this risk.</p>
         </description>
         <origin>
            <actor type="party" actor-uuid="49f73135-efab-4275-9a79-
003656ad890a"></actor>
         </origin>

         <required-asset uuid="7bd1a61e-4fda-4c52-a447-14072ef6e042">
            <subject subject-uuid="6e0d71b5-3dac-4a9b-b60d-da61b95eccb9" type="party" />
            <subject subject-uuid="6e0d71b5-3dac-4a9b-b60d-da61b95eccb9" type="party" />
            <description><p>Describe required resources.</p></description>
         </required-asset>
      </response>
   </risk>
```



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/reference/datatypes/#markup-line

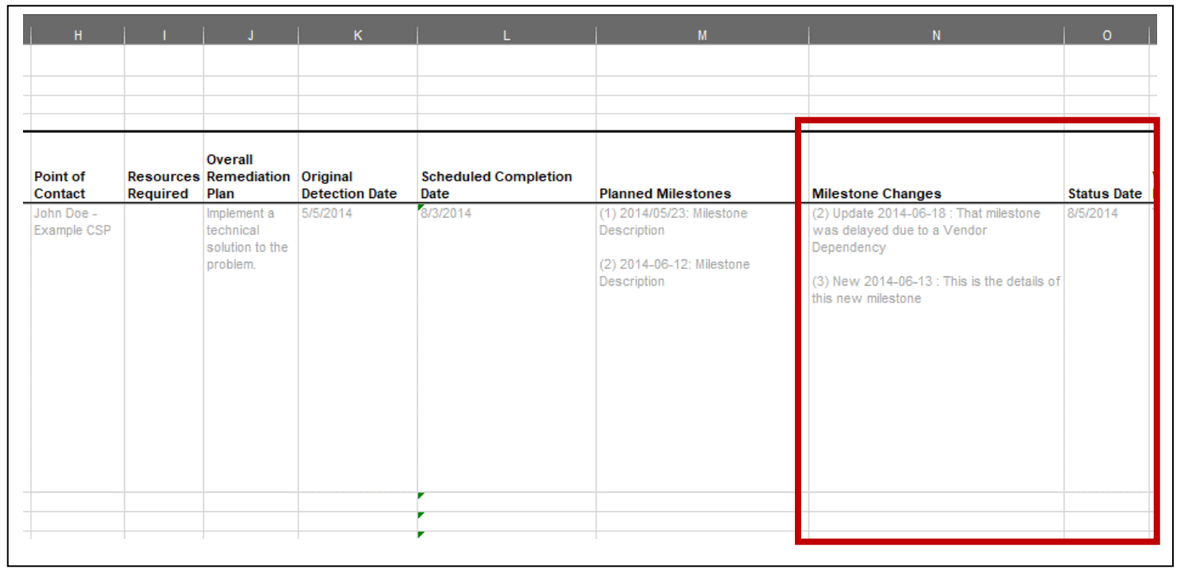
4.3.1. Planned Remediation Schedule

The Planned Milestones are identified within the `response` assembly using the `task` assemblies. There must be at least one `task` assembly of `type` "milestone. There may be additional `tasks` assemblies of `type` "action" or "milestone". A POA&M tool should offer the option of viewing either just the milestones or all actions and milestones.

Each `task` assembly must have a `title` field that briefly names the milestone and a `description` field. OSCAL requires the description field to be present; however, FedRAMP allows it to be empty. The timing assembly must be present with a `within-date-range` field. The Scheduled Completion Date for the POA&M item is the value of the `end` field farthest in the future.

Representation

```
<risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
  <!-- title, description, statement, status, characterization -->
  <response uuid="e9ee6fe2-856f-42c7-8c2e-ff6466d31010" lifecycle="planned">
    <title>CSP's Remediation Plan</title>
    <description>
      <p>Describe the CSP's intended approach to remediating this risk.</p>
    </description>
    <origin>
      <actor type="party" uuid-ref="49f73135-efab-4275-9a79-003656ad890a"></actor>
    </origin>

    <required-asset uuid="7bd1a61e-4fda-4c52-a447-14072ef6e042">
      <subject subject-uuid="6e0d71b5-3dac-4a9b-b60d-da61b95eccb9" type="party" />
      <subject subject-uuid="6e0d71b5-3dac-4a9b-b60d-da61b95eccb9" type="party" />
      <description><p>Describe required resources.</p></description>
    </required-asset>
    <task uuid="a12dea1d-e4d1-4f09-aacf-1eaf203a3092" type="milestone">
      <title>[Example]Milestone 1</title>
      <description><p>Optional description</p></description>
      <timing>
        <within-date-range start="2020-07-01T00:00:00Z"
                           end="2020-07-02T00:00:00Z"/>
      </timing>
    </task>
    <task uuid="08c50f90-3b08-49fd-862d-32ec96e6bee5" type="milestone">
      <title>[Example]Milestone 2</title>
      <description><p>Optional description</p></description>
      <timing>
        <within-date-range start="2020-07-05T00:00:00Z"
                           end="2020-07-07T00:00:00Z"/>
      </timing>
    </task>
  </response>                    <!-- remediation-tracking -->
</risk>
```



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

4.4. Risk Tracking

Tracking is initiated by adding the `risk-log` assembly to the `risk` assembly, which must have one or more `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 entry assemblies.

Each `entry` assembly must have a `title`, `description` , and `start` field. There may also be an `end`, `logged-by`, and `related-response` fields. If the `end` field is missing it is presumed to have the same value as the `start` field. The logged-by field is optional and contains the uuid of the person (party) who made the entry. The related-response field is optional and contains the UUID of the

For performed actions, `start` should reflect when the action was performed. For status updates, this should reflect the effective date of the status information. OSCAL requires the `description` field to be present, but FedRAMP allows it to 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 `type` tag of "`risk-tracking`".

Representation

```
<risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
   <!-- title, description, statement, status, response -->
   <risk-log>
      <entry uuid="1b500d56-1936-41eb-8b60-a2984937ab89">
         <title>Activity 1</title>
         <description />
         <start>2020-07-02T00:00:00Z</start>
         <end>2020-08-02T00:00:00Z</end>
         <logged-by party-uuid=""/>
         <related-response response-uuid="e9ee6fe2-856f-42c7-8c2e-ff6466d31010">
            <related-task task-uuid="a12dea1d-e4d1-4f09-aacf-1eaf203a3092" />
         </related-response>
      </entry>
      <entry uuid="316fb3fe-927a-49a1-9a72-a58722862623">
         <title>Activity 2</title>
         <description />
         <start>2020-07-07T00:00:00Z</start>
      </entry>
      <entry uuid="d084a039-bdd1-4ccd-a06a-53355e07fa2f">
         <title>Vendor Check-in</title>
         <description><p>Description of the result of the vendor check-in.</p></description>
         <start>2020-07-07T00:00:00Z</start>
         <prop name='conformity' ns='https://fedramp.gov/ns/oscal'>vendor-check-in</prop>
      </entry>
      <entry uuid="0b09e341-cf3c-4de7-b728-751c6e88b653">
         <title>Risk Closed</title>
         <description>
            <p>Describe what action(s) the CSP took to close the risk.</p>
            <p>[EXAMPLE]Applied patch. Vulnerability no longer found in subsequent scan.</p>
         </description>
         <start>2020-07-07T00:00:00Z</start>
         <status-change>closed</status-change>
      </entry>
   </risk-log>
</risk>
```

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 original risk information is not modified. Additional content is added to identify these changes. Typically, an additional `observation` is added and linked to the `poam-item`, and additional `facet` fields are added to the `risk` assembly. There may be both Operational Requirement (OR) and Risk Assessment (RA) information in the same `risk` assembly, each with its own `observation`.

4.5.1. False Positive (FP)

To initially identify a false positive, add a "false-positive" FedRAMP Extension property to the `risk` field and set its value to "investigating". Once evidence is identified to support the FP, change the risk assembly's "false-positive" value to "pending" and add an `observation` with the `type` field set to "false-positive". Typically, the `method` is set to "EXAMINE". Add an additional `related-observation` field linking the `poam-item` to the new observation.

Once the FP is approved, change the "false-positive" extension's value to "approved" and close the risk as described in *Section 4.6, Risk Closure*.

Representation

```
<observation uuid="46209140-8263-4e74-b3c9-cead4ffed22c">
   <title>False Positive</title>
   <description><p>Describe the false positive here.</p></description>
   <method>EXAMINE</method>
   <type>false-positive</type>
   <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/article/describing/something.htm">
      <description><p>Vendor detail describing why this happens.</p></description>
   </relevant-evidence>
   <collected>2020-10-10T00:00:00Z</collected>
</observation>

<risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
   <title>Vulnerability Title</title>
   <description><p>Vulnerability description</p></description>
   <statement><p>Risk statement.</p></statement>
   <prop name="impacted-control-id"     ns="https://fedramp.gov/ns/oscal">ac-2</prop>
   <prop name="vendor-dependency"       ns="https://fedramp.gov/ns/oscal">tracking</prop>
   <prop name="operational-requirement" ns="https://fedramp.gov/ns/oscal">approved</prop>
   <prop name="false-positive"          ns="https://fedramp.gov/ns/oscal">withdrawn</prop>
   <prop name="risk-adjustment"         ns="https://fedramp.gov/ns/oscal">approved</prop>
   <status>open</status>
</risk>

<poam-item uuid="6F5FFF73-CAC6-4DA0-A0D9-0F931A5EFAFA">
   <!-- cut -->
   <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
   <related-observation observation-uuid="46209140-8263-4e74-b3c9-cead4ffed22c" />
   <associated-risk risk-uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7" />
</poam-item>
```

Add an entry to the risk log when investigating, as well as for submission and approval events respectively.

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

4.5.2. Operationally Required (OR)

To initially identify an OR, add an "operational-requirement" FedRAMP Extension property to the `risk` field and set its value to "investigating". Once evidence is identified to support the OR, change the risk assembly's "operational-requirement" value to "pending" and add an `observation` with the `type` field set to "operational-requirement". Typically, the `method` is set to `EXAMINE`; however, another method may be identified if more appropriate. Add an additional `related-observation` field linking the `poam-item` to the new observation.

Once the OR is approved, change the "operational-requirement" extension value to "approved".

If a risk adjustment is also required for OR approval (such as FedRAMP requires for High ORs), simply also follow the instructions in the next section for risk adjustments. When there is both an OR and an RA, each will have their own `observation` assembly and respective `related-observation` entries in the poam-item assembly.

Representation

```
<observation uuid="46209140-8263-4e74-b3c9-cead4ffed22c">
   <title>Operational Requirement</title>
   <description><p>Provide the justification for the OR.</p></description>
   <method>EXAMINE</method>
   <type>operational-requirement</type>
   <relevant-evidence href="#53af7193-b25d-4ed2-a82f-5954d2d0df61">
      <description><p>A screen shot showing impact when patch is applied.</p></description>
   </relevant-evidence>
   <relevant-evidence href="https://vendor.site/article/describing/something.html">
      <description><p>Vendor detail describing why this happens.</p></description>
   </relevant-evidence>
   <collected>2020-10-10T00:00:00Z</collected>
</observation>

<risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
   <title>Vulnerability Title</title>
   <description><p>Vulnerability description</p></description>
   <statement><p>Risk statement.</p></statement>
   <prop name="impacted-control-id"     ns="https://fedramp.gov/ns/oscal">ac-2</prop>
   <prop name="operational-requirement" ns="https://fedramp.gov/ns/oscal">approved</prop>
   <status>open</status>
</risk>

<poam-item uuid="6F5FFF73-CAC6-4DA0-A0D9-0F931A5EFAFA">
   <!-- cut -->
   <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
   <related-observation observation-uuid="46209140-8263-4e74-b3c9-cead4ffed22c" />
   <associated-risk risk-uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7" />
</poam-item>
```

Add an entry to the risk log when investigating, as well as for submission and approval events respectively.

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/reference/datatypes/#markup-line

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:

```
<facet name="likelihood" value="high" system="https://fedramp.gov">
   <annotation name="state" value="initial" />
</facet>
<facet name="impact" value="high" system="https://fedramp.gov">
   <annotation name="state" value="initial" />
</facet>
```

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**:

```
<facet name="likelihood" value="low" system="https://fedramp.gov">
   <annotation name="state" value="adjusted" />
</facet>
<facet name="impact" value="moderate" system="https://fedramp.gov">
   <annotation name="state" value="adjusted" />
</facet>
```

Add an entry to the risk log when investigating, for the completion of each mitigating factor's implementation (if appropriate), as well as for submission and approval events respectively.

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/reference/datatypes/#markup-line

4.5.3. Risk Adjustment (RA)

To initially identify an RA, add a "risk-adjustment" FedRAMP Extension property to the `risk` field and set its value to "investigating". Once evidence is identified or mitigating factors are implemented, change the risk assembly's "risk-adjustment" value to "pending" and add an `observation` with the `type` field set to "risk-adjustment". Typically, the `method` is set to `EXAMINE`; however, another method may be identified if more appropriate. Add an additional `related-observation` field linking the `poam-item` to the new observation.

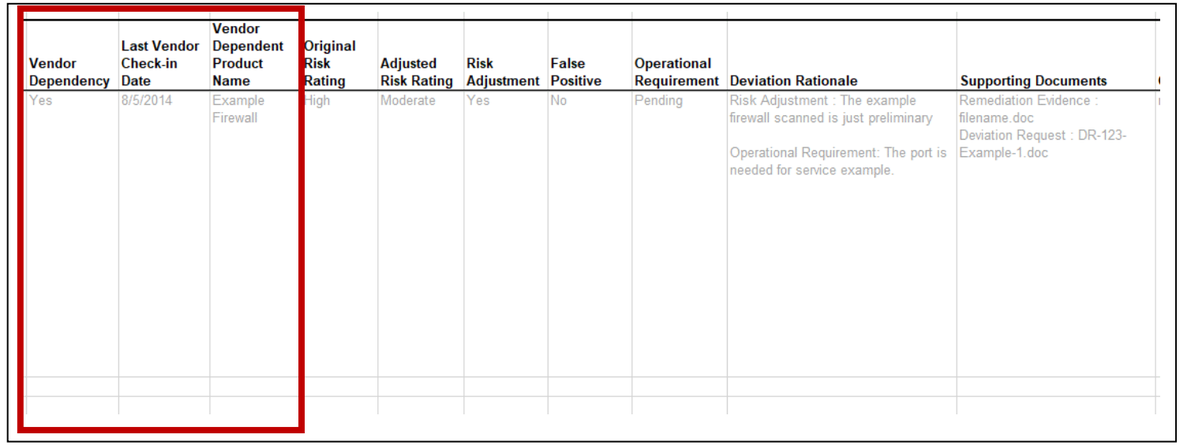
As mitigating factors are identified or implemented, add `mitigating-factor` assemblies to the `risk` assembly. There must be at least one mitigating factor for an RA. Based on those factors, add additional `facet` assemblies with adjusted risk values.

Once the RA is approved, change the "risk-adjustment" extension value to "approved".

If the RA is performed in concert with an OR (such as FedRAMP requires for High ORs), simply also follow the instructions in the previous section for operationally required risks. When there is both an OR and an RA, each will have their own `observation` assembly and respective `related-observation` entries in the poam-item assembly.

Representation

```
<observation uuid="46209140-8263-4e74-b3c9-cead4ffed22c">
   <type>risk-adjustment</type>
   <relevant-evidence>
      <description>
         <p>Describe the risk adjustment evidence here.</p>
      </description>
      <link href="#53af7193-b25d-4ed2-a82f-5954d2d0df61" rel="evidence"/>
      </remarks>
   </relevant-evidence>
   <collected>2020-10-10T00:00:00Z</collected>
</observation>
<risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
   <prop name="risk-adjustment"          ns="https://fedramp.gov/ns/oscal">approved</prop>
   <characterization>
      <facet name="likelihood" value="high" system="https://fedramp.gov">
         <annotation name="state" value="initial" />
      </facet>
      <facet name="impact" value="high" system="https://fedramp.gov">
         <annotation name="state" value="initial" />
      </facet>
      <facet name="likelihood" value="moderate" system="https://fedramp.gov">
         <annotation name="state" value="adjusted">
            <remarks>
               <p>Explain why likelihood was adjusted.</p>
            </remarks>
         </annotation>
      </facet>
      <facet name="impact" value="low" system="https://fedramp.gov">
         <annotation name="state" value="adjusted">
            <remarks>
               <p>Explain why impact was adjusted.</p>
            </remarks>
         </annotation>
      </facet>
   </characterization>
   <mitigating-factor uuid="260d3c0a-fc2e-4627-9fb9-a003acdc4b14">
      <description><p>Describe mitigating factor</p></description>
   </mitigating-factor>
</risk>
<poam-item uuid="6F5FFF73-CAC6-4DA0-A0D9-0F931A5EFAFA">
   <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
   <related-observation observation-uuid="46209140-8263-4e74-b3c9-cead4ffed22c" />
   <associated-risk risk-uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7" />
</poam-item>
```



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/reference/datatypes/#markup-line

4.5.4. Vendor Dependency

To initially identify a vendor dependency, add a "vendor-dependency" FedRAMP Extension property to the `risk` field and set its value to "investigating". Once evidence is identified to support the dependency, change the risk assembly's "vendor-dependency" value to "tracking" and add an `observation` with the `type` field set to "vendor-dependency". Typically, the `method` is set to `EXAMINE`; however, another method may be identified if more appropriate. Add an additional `related-observation` field linking the `poam-item` to the new observation.

Within the `observation` assembly, explain the dependency in the `description` field. The `observation` assembly must include a `subject-reference` identifying the component or inventory-item. The Vendor Dependency Product Name is provided from the component or inventory-item details.

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`.)

Once the vendor publishes a resolution, change the "vendor-dependency" extension value to "resolved".

Representation

```
<observation uuid="46209140-8263-4e74-b3c9-cead4ffed22c">
   <title>Vendor Dependency</title>
   <description><p>Describe the vendor dependency here.</p></description>
   <method>INTERVIEW</method>
   <type>vendor-dependency</type>
   <subject subject-uuid="a49ed61e-fca1-4ffa-b5e7-c23a2375a7a0" type="component" />
   <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/article/describing/something.htm">
      <description><p>Vendor detail describing why this happens.</p></description>
   </relevant-evidence>
   <collected>2020-10-10T00:00:00Z</collected>
</observation>

<risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
   <title>Vulnerability Title</title>
   <description><p>Vulnerability description</p></description>
   <statement><p>Risk statement.</p></statement>
   <prop name="impacted-control-id"     ns="https://fedramp.gov/ns/oscal">ac-2</prop>
   <prop name="vendor-dependency"       ns="https://fedramp.gov/ns/oscal">tracking</prop>
   <status>open</status>
</risk>

<poam-item uuid="6F5FFF73-CAC6-4DA0-A0D9-0F931A5EFAFA">
   <!-- cut -->
   <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
   <related-observation observation-uuid="46209140-8263-4e74-b3c9-cead4ffed22c" />
   <associated-risk risk-uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7" />
</poam-item>
```

Add an entry to the risk log when investigating, as well as for each vendor check-in. As the CSP performs the required regular vendor check-ins, each must be added to the `risk-log` assembly as an additional `entry`. The `title` should be set to "`Vendor Check-in`", the `start` field must indicate when the check-in occurred. The result of the check-in must be described in the `description` field.

When the vendor publishes the resolution, add another risk log entry reflecting the date the resolution was published.

[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`.

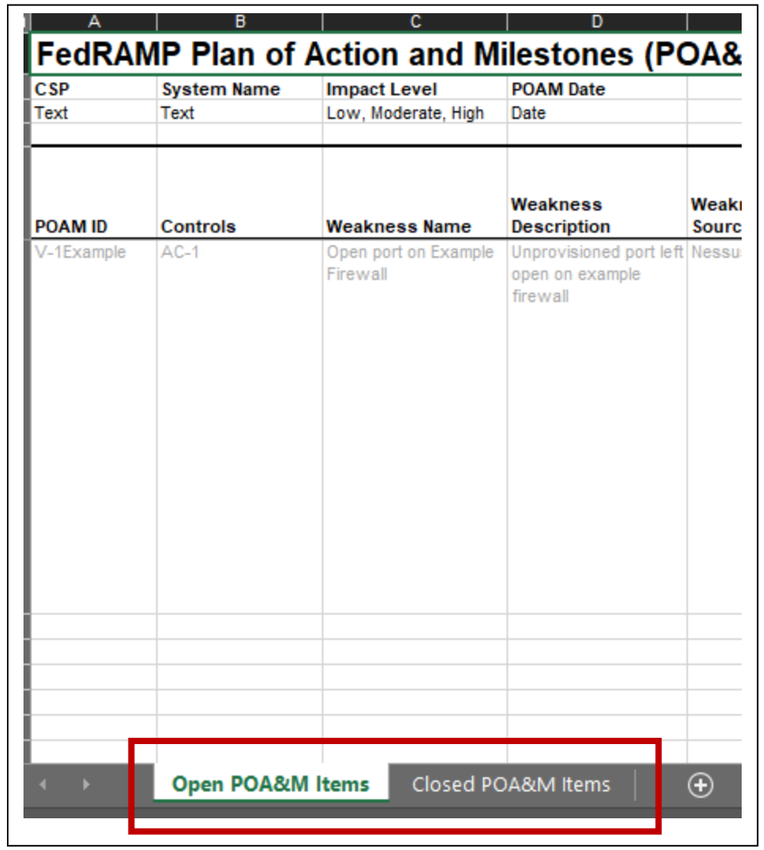
Evidence may be cited from an `observation` as `relative-evidence`.

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/reference/datatypes/#markup-line

4.6. Risk Closure

When a risk is closed through remediation or false-positive approval, they must be closed. The risk should remain in the POA&M with the following changes.

First, in the `risk` assembly, change the `status` field to "`closed`". Then make a final entry in the `risk-log` assembly. In the `entry` assembly summarize the reason for closure in the `description` field, set the `start` field to indicate the date of closure, and the `status-change` field to "closed". Individual actions performed for closure should each have their own entries in the risk log.

If it is appropriate to attach evidence of closure, add an `observation` assembly with the `type` field set to "closure", and cite the appropriate evidence.

Representation

```
<observation uuid="46209140-8263-4e74-b3c9-cead4ffed22c">
   <title>Risk Closure</title>
   <description><p>Describe the closure evidence here.</p></description>
   <method>EXAMINE</method>
   <type>closure</type>
   <subject subject-uuid="a49ed61e-fca1-4ffa-b5e7-c23a2375a7a0" type="component" />
   <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/article/describing/something.htm">
      <description><p>Vendor detail describing why this happens.</p></description>
   </relevant-evidence>
   <collected>2020-10-10T00:00:00Z</collected>
</observation>

<risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
  <!-- title, description, statement, status, mitigation, response -->
   <risk-log>
      <entry uuid="1b500d56-1936-41eb-8b60-a2984937ab89">
      </entry>
      <entry uuid="316fb3fe-927a-49a1-9a72-a58722862623">
      </entry>
      <entry uuid="d084a039-bdd1-4ccd-a06a-53355e07fa2f">
      </entry>
      <entry uuid="0b09e341-cf3c-4de7-b728-751c6e88b653">
         <title>Risk Closed</title>
         <description>
            <p>Describe what action(s) the CSP took to close the risk.</p>
            <p>[EXAMPLE]Applied patch. Vulnerability no longer found in subsequent
scan.</p>
         </description>
         <start>2020-07-07T00:00:00Z</start>
         <status-change>closed</status-change>
      </entry>
   </risk-log>
</risk>
<poam-item uuid="6F5FFF73-CAC6-4DA0-A0D9-0F931A5EFAFA">
   <!-- cut -->
   <related-observation observation-uuid="0aa54106-8a63-4953-ac0d-30ff91f8d4ab" />
   <related-observation observation-uuid="46209140-8263-4e74-b3c9-cead4ffed22c" />
   <associated-risk risk-uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7" />
</poam-item>
```

APPENDIX A. CVSS SCORING

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

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 `system` value of "http://www.first.org/cvss/v3.1".

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

```
<risk id="risk-3-1">
  <!-- title, description, statement, status -->
   <characterization>
      <origin>
         <actor type="party" uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
      </origin>

       <!-- CVSS Metrics using V3.1 using abbreviations -->
      <facet name="AV" system="http://www.first.org/cvss/v3.1" value="network"/>
      <facet name="AC" system="http://www.first.org/cvss/v3.1" value="high"/>
      <facet name="PR" system="http://www.first.org/cvss/v3.1" value="low"/>

       <!-- CVSS Metrics using V3.1 using names -->
      <facet name="access-vector"       system="http://www.first.org/cvss/v3.1"
                                        value="network"/>

      <facet name="access-complexity"   system="http://www.first.org/cvss/v3.1"
                                        value="high"/>

      <facet name="privileges-required" system="http://www.first.org/cvss/v3.1"
                                        value="low"/>
   </characterization>
</risk>
```