GUIDE TO OSCAL-BASED FEDRAMP SECURITY ASSESSMENT PLANS (SAP)

fedramp1.0.0-oscal1.0.0

July 6, 2021

FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
8/1/2020	Initial Publication	1.0	FedRAMP PMO
2/25/2021	Updated to align with RC-2 syntax	2.0	FedRAMP PMO
7/6/2021	Finalize alignment with OSCAL 1.0.0 syntax updates, update versioning scheme to match release strategy guidance.	fedramp1.0.0-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

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 Plans (SAPs) content.

It provides guidance and examples intended to guide an organization in the production and use of OSCAL-based FedRAMP-compliant SAP 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 SAP 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 Plans.

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 SAP 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.

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 and allowed 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 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 SAP 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.

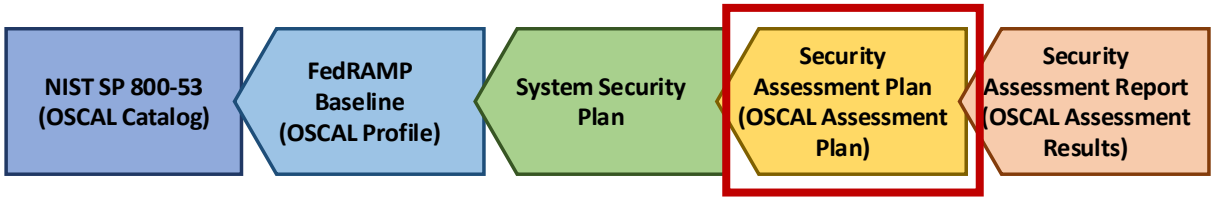
3.1. XML and JSON Formats

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

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

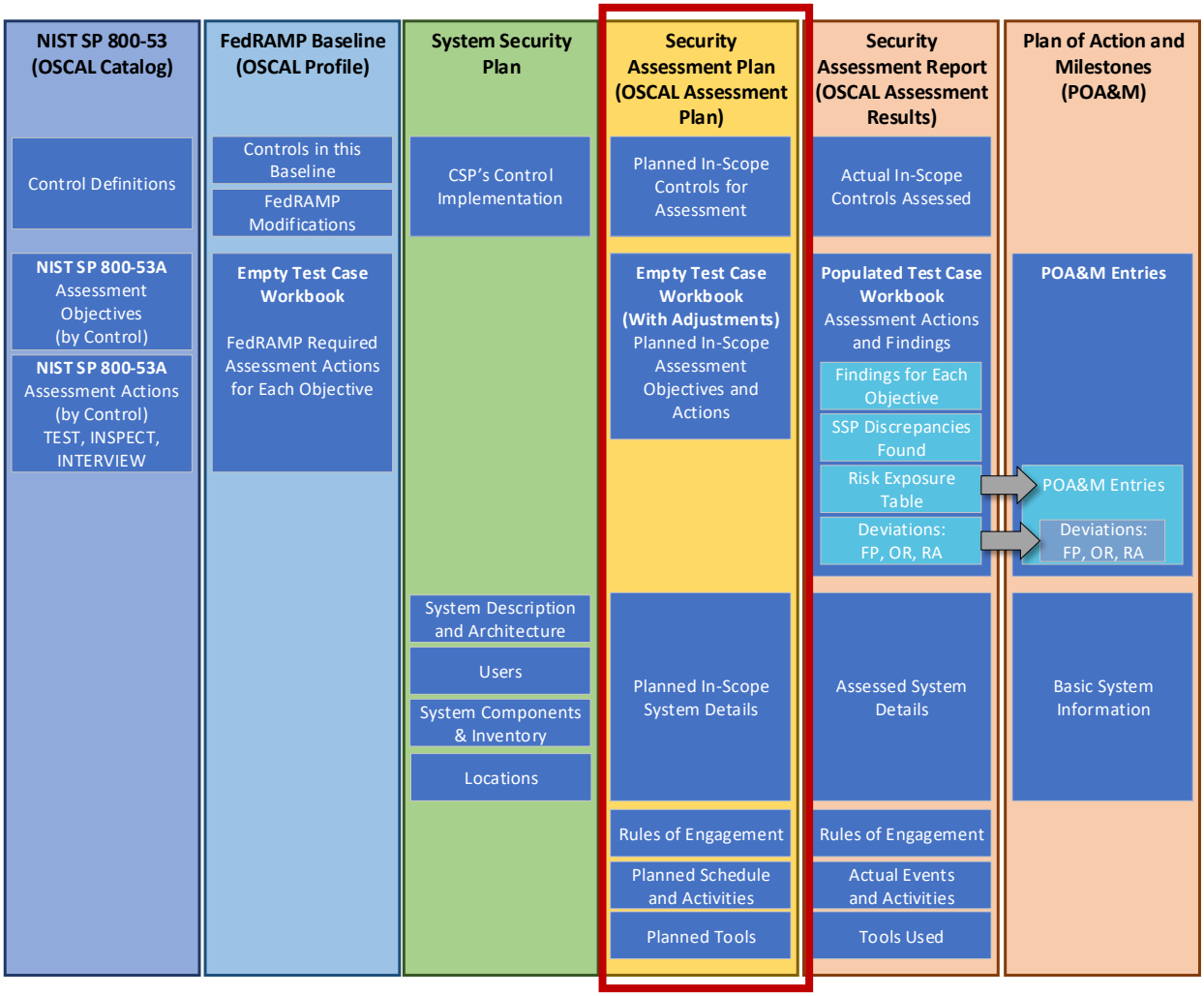
3.2. SAP File Concepts

Unlike the traditional MS Word-based SSP, SAP, and SAR, 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 assessment objectives and actions that appear in a blank test case workbook (TCW), are defined in the FedRAMP profile, and simply referenced by the SAP and SAR. Only deviations from the TCW are captured in the SAP or SAR.



Baseline and SSP Information is referenced instead of duplicated.

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

The SAP also inherits the SSP's pointer to the appropriate OSCAL-based FedRAMP Baseline. Through that linkage, the SAP references the assessment objectives and actions typically identified in the FedRAMP TCW.

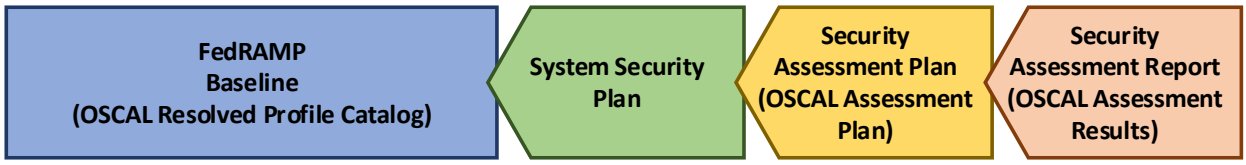
The only reason to include this content in the SAP is when the assessor documents a deviation from the SSP, Baseline, or TCW.

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 SAP Template

FedRAMP offers an OSCAL-based SAP 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 SAP Template is available in XML and JSON formats here:

- OSCAL-based FedRAMP SAP Template (JSON Format): https://github.com/GSA/fedramp-automation/raw/master/templates/sap/json/FedRAMP-SAP-OSCAL-Template.json
- OSCAL-based FedRAMP SAP Template (XML Format): https://github.com/GSA/fedramp-automation/raw/master/templates/sap/xml/FedRAMP-SAP-OSCAL-Template.xml

3.4. OSCAL's SAP Minimum File Requirements

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

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

3.5. Importing the System Security Plan

OSCAL is designed for traceability. Because of this, the assessment plan is designed to be linked to the system security plan. Rather than duplicating content from the SSP, the SAP is intended to reference the SSP content itself. **If a system security plan is available in OSCAL format, it must be used with the OSCAL-based security assessment plan.**

Unavailable or Inaccurate OSCAL-based SSP Content

FedRAMP enables an assessor to use the OSCAL-based SSP, when no OSCAL-based SSP exists, or where the assessor finds it to be inaccurate. Where available, this guide explains how to capture relevant system information directly in the OSCAL SAP when needed. ***Assessors must only use this capability to address unavailable or inaccurate content and must not duplicate accurate SSP content into the SAP.***

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-of-resource]" />
```

XPath Queries

```
(SAP) 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 2.7, Citations and Attachments in OSCAL Files*, for guidance on handling.

SAP Back Matter Representation

```
<back-matter>
   <resource uuid="96445439-6ce1-4e22-beae-aa72cfe173d0">
      <title>[System Name] [FIPS-199 Level] SSP</title>
      <prop name="type" name="system-security-plan"/>
      <!-- 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 SAP

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

XPath Queries

```
(SAP) Referenced OSCAL-based SSP

XML:
  /*/back-matter/resource[@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
```

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

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

3.5.1. When OSCAL-based SSP Information is Inaccurate

When an assessor encounters inaccurate information in an OSCAL-based SSP, they should encourage the CSP to fix it and use the corrected version of the SSP. The CSP is responsible for all SSP content. An assessor's tools must not change an SSP.

If an assessor must move forward with inaccurate SSP information, the SAP syntax allows for SSP information correction. Performing these corrections in the SAP instead of the SSP, ensures the corrected content is clearly attributed to the assessor.

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

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

The OSCAL-based SAP must always have an `import-ssp` field, even if no OSCAL-based SSP is available. To compensate for this, use a URI fragment that points to a `resource` in the `back-matter`. The resource must have a "type" property with the value of **`no-oscal-ssp`**

SAP Representation

```
<import-ssp href="#7c30125f-c056-4888-9f1a-7ed1b6a1b638" />

<back-matter>
   <resource id="ssp-information">
      <title>System's Full Name</title>
      <description>
         <p>Briefly describe the system. This will appear in the SAR.</p>
      </description>
         <prop name="type" value="no-oscal-ssp"/>
         <prop name="type" value="system-security-plan"/>
         <prop name="title-short"
            ns="https://fedramp.gov/ns/oscal" value="SFN"/>
         <prop name="authorization-date"
            ns="https://fedramp.gov/ns/oscal" value="2017-01-02T00:00:00Z"/>
         <prop name="system-id"
            ns="https://fedramp.gov/ns/oscal" value="FR00000000"/>
         <prop name="import-profile" ns="https://fedramp.gov/ns/oscal"
                                              value="#uuid-of-resource"/>
         <prop name="purpose" ns="https://fedramp.gov/ns/oscal"
          value="Briefly state the system's purpose, for the SAP and SAR."/>
         <rlink href="/documents/CSP_System_SSP.docx" media-type="-cut-"/>
   </resource>
</back-matter>
```

XPath Queries

```
(SAP) Resource representing system details when no OSCAL-based SSP exists:
  /*/back-matter/resource/prop[@name='type'][@value='no-oscal-ssp']
```

The system's authorization date, purpose, and description have not historically been displayed in the SAP, but must be present in the SAP for the SAR to reference.

Include the system name in the `title` field, and the system description in the `description` field. Add FedRAMP Extension properties to capture the system's short name as "title-short", FedRAMP-assigned system identifier as "system-id", and describe the system's purpose in "purpose".

Also include the "import-profile" extension and supply either a URI to the profile externally, or a URI fragment with the UUID of the SAP resource containing the relevant profile details.

In addition to defining the system here, SAP tools must place other relevant SSP information in the SAP's `metadata` and `local-definitions` section as needed for the SAP to reference this information, essentially treating all relevant SSP content as "missing" from an OSCAL perspective.

The relevant sections of this guide describe how to represent missing SSP in formation in the SAP when needed.

4. SAP TEMPLATE TO OSCAL MAPPING

For SAP-specific content, each page of the SAP is represented in this section, along with OSCAL code snippets for representing the information in OSCAL syntax. There is also XPath syntax for querying the code in an OSCAL-based FedRAMP SAP represented in XML format.

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*

It is not necessary to represent the following sections of the SAR template in OSCAL; however, tools should present users with this content where it is appropriate:

- Any blue-text instructions found in the SAP template, where the instructions are related to the content itself.
- Table of Contents
- Introductory and instructive content in each section.

The Annual SAP was used, which includes all information typically found in the Initial SAP, plus a scope section that is unique to annual assessments. OSCAL always requires a scope. For initial assessments, the scope is all controls. For annual assessments, it is the controls required by FedRAMP.

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

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

2. SCOPE

This SAP must specifically address the controls for Annual Assessment. The scope of the security tests that will be performed for the CSP service offering is limited and well defined. Tests on systems and interfaces that are outside the boundary of the CSP service offering (for FedRAMP) are not included in this plan.

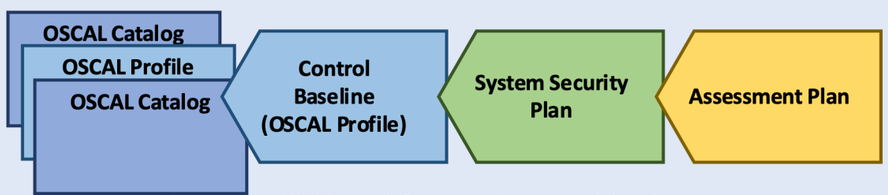
The scope for this annual assessment is limited to controls that are part of FedRAMP's continuous monitoring, plus controls referenced in the POA&M from the previous assessment, plus other controls selected by the authorizing official. All components of the numbered controls listed in the table will be tested. This annual assessment's in-scope set of controls is roughly one third of all FedRAMP (NIST 800-53 Rev 3) security controls. The agreed set is as follows:

Control Family	Controls to be Assessed

IMPORTANT

SAP tools must import (open) the OSCAL-based SSP, then use the SSP content to import (open) the FedRAMP Control Baseline (profile). It may also be necessary to open any catalogs or additional profiles called by the SSP's profile.

This provides access to all controls in the baseline, including control objectives, and control assessment activities, as well as any FedRAMP modifications. To reduce processing, a tool may link to a "resolved profile catalog" version of the baseline, which represents a pre-processing of the profile and catalog data.



Traverse the OSCAL stack for control scope and details.

Control selection is limited in scope to the controls resulting from the SSP's profile.
An OSCAL SAP may not include any control outside of this scope.

HELPFUL HINT

When processing an OSCAL-based FedRAMP baseline (profile or resolved-profile-catalog) for annual assessment inclusion, the FedRAMP core/critical controls are identified with the FedRAMP Extension, "CORE". (`<prop name='CORE' ns='https://fedramp.gov/ns/oscal' value='true'/>`)

4.1. SAP Scope

With FedRAMP legacy templates, the *Scope* section was only found in the template for the annual assessment. This is because the initial assessment requires all controls to be included. An OSCAL SAP must always explicitly select the in-scope controls from the applicable FedRAMP Baseline/Profile. For initial assessments, this can be as simple as specifying `include-all`. For annual assessments, use `include-control` instead - one for each control included in the assessment. Controls may also be explicitly excluded from the control scope.

Representation

```
<!-- metadata -->

<reviewed-controls>
   <control-selection>
      <description>
         <p>Include all controls in the baseline.</p>
         <p>Then exclude any specific controls if necessary.</p>
         <p>Provide rationale/justification for control exclusion here.</p>
      </description>

      <include-all />
      <exclude-control control-id="ac-1" />
      <!-- OR -->
      <include-control control-id="ac-2" />
      <include-control control-id="ac-3" />
      <!-- repeat as needed for each control -->

   </controls>
   <!-- control-objectives -->
   <!-- objectives -->
</objectives>
<!-- assessment-subject -->
```

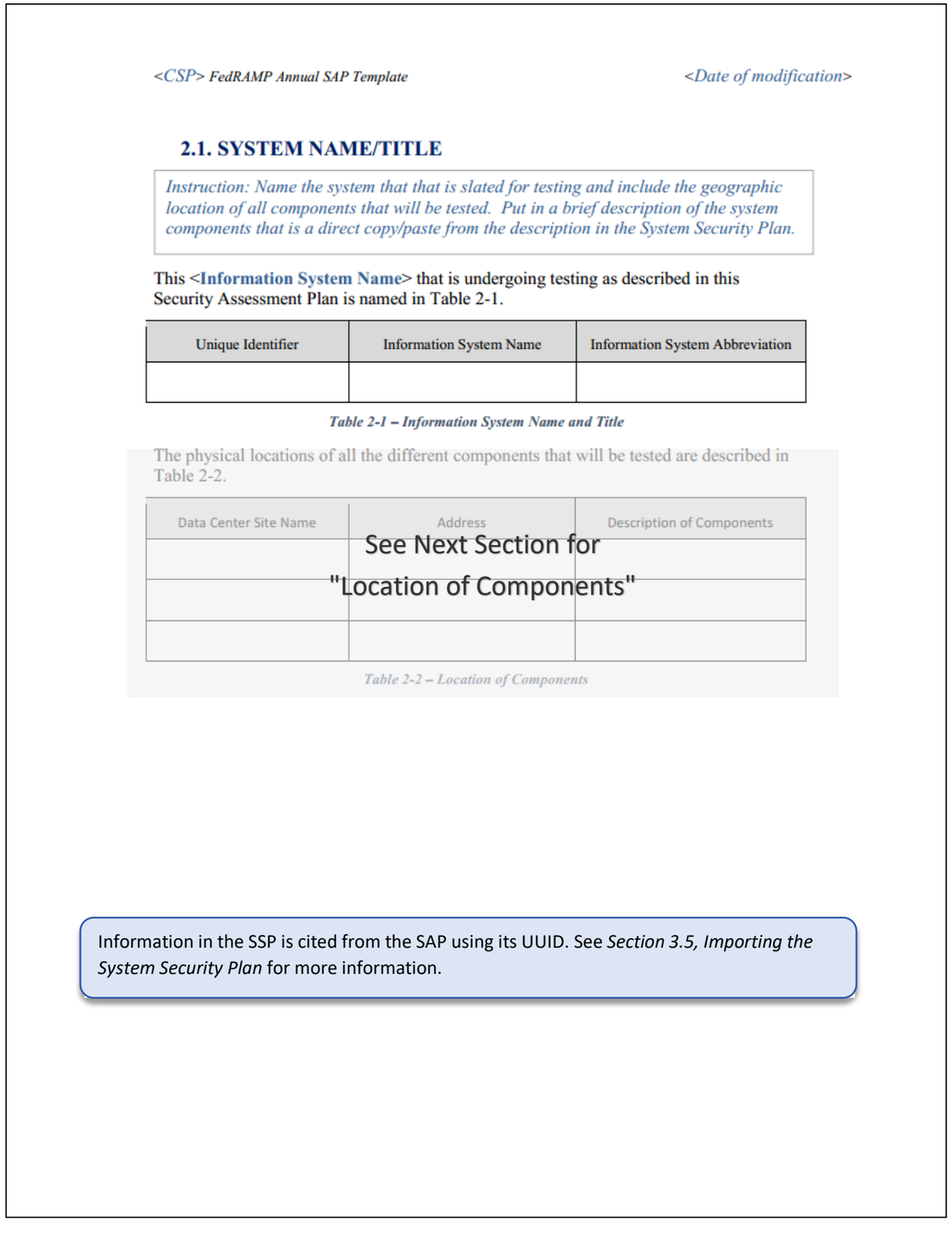
XPath Queries

```
(SAP) Include All Controls? (true or false):
  boolean(/*/objectives/controls/include-all)

(SAP) Exclude Controls Specified? (true or false):
  boolean(/*/objectives/controls/exclude-control)

(SAP) Exclude Controls Total (integer):
  count(/*/objectives/controls/exclude-control)

(SAP) Exclude Specific Control (string):
  /*/objectives/controls/exclude-control[1]/@control-id

NOTE: Replace "exclude-control" with "include-control" above for any explicitly included
  controls; however, this is redundant when used with 'all'.
```

Replace "[1]" with "[2]", "[3]", etc.

NOTES:

- Tools should validate the control IDs for explicitly included or excluded controls using the relevant baseline.
- FedRAMP's guidance and requirements regarding which controls are in-scope for each assessment does not change with OSCAL.



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

2.1. SYSTEM NAME/TITLE

Instruction: Name the system that that is slated for testing and include the geographic location of all components that will be tested. Put in a brief description of the system components that is a direct copy/paste from the description in the System Security Plan.

This <**Information System Name**> that is undergoing testing as described in this Security Assessment Plan is named in Table 2-1.

Unique Identifier	Information System Name	Information System Abbreviation

Table 2-1 – Information System Name and Title

The physical locations of all the different components that will be tested are described in Table 2-2.

Data Center Site Name	Address	Description of Components

Table 2-2 – Location of Components

See Next Section for "Location of Components"

Information in the SSP is cited from the SAP using its UUID. See *Section 3.5, Importing the System Security Plan* for more information.

4.2. SAP System Name/Title

This information should come entirely from the imported SSP. If the OSCAL-based SSP exists and is accurate, the tool should query that file for this information as follows:

SSP XPath Queries

Table 2-1

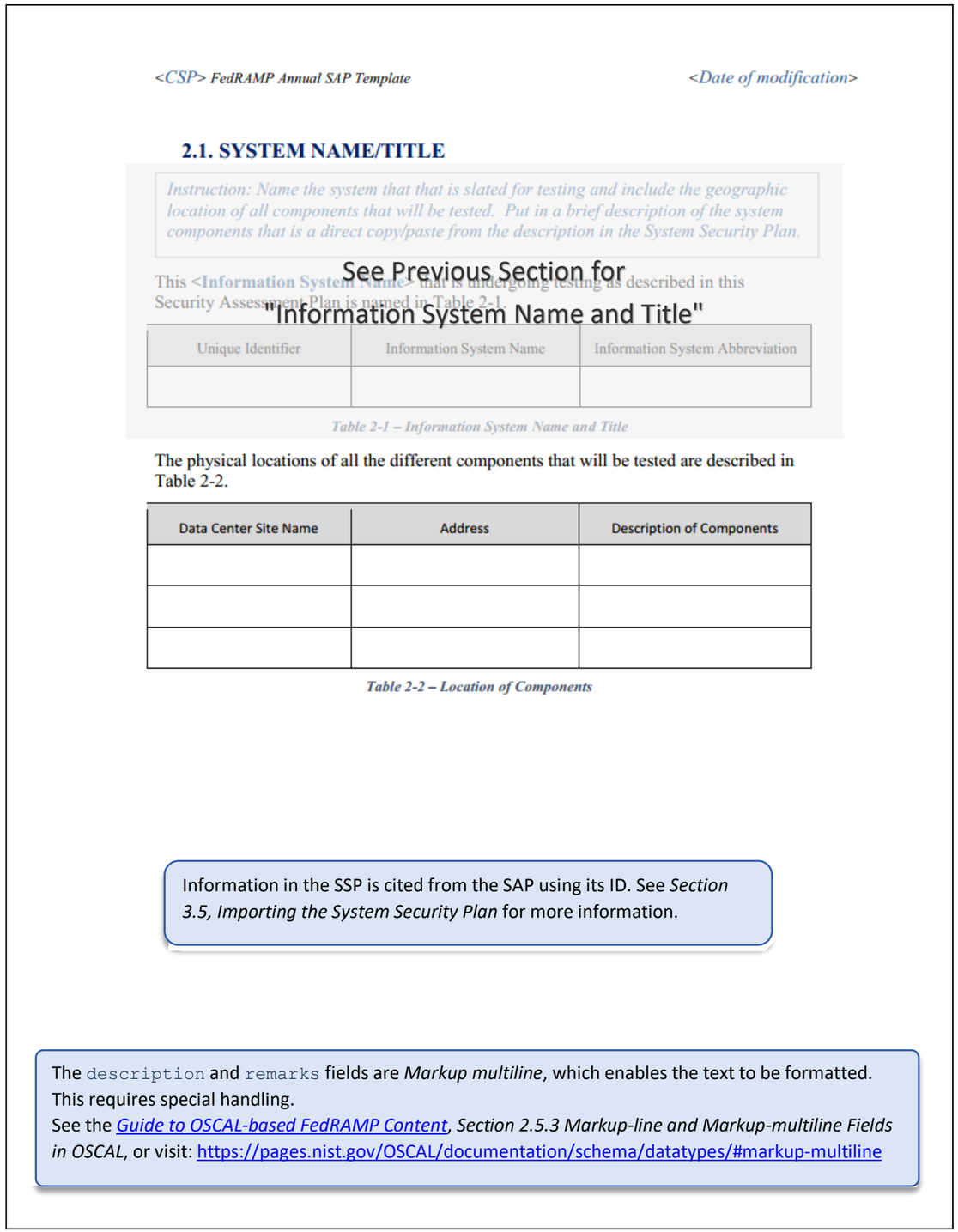
```
(SSP) Unique Identifier:
  /*/system-characteristics/system-id[@identifier-type='https://fedramp.gov']
(SSP) Information System Name:
  /*/system-characteristics/system-name
(SSP) Information System Abbreviation:
  /*/system-characteristics/system-name-short
```

4.2.1. If No OSCAL-based SSP Exists (System Name/Title)

If no OSCAL-based SSP exists, as described in *Section 3.5.2, If No OSCAL-based SSP Exists (General)*, the resource with the `no-oscal-ssp` type must designate the system's identifier, name, and abbreviation.

NOTES:

- The system's authorization date, purpose, and description have not historically been displayed sin the SAP, but must be present when the SAR references this content.



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

2.1. SYSTEM NAME/TITLE

Instruction: Name the system that that is slated for testing and include the geographic location of all components that will be tested. Put in a brief description of the system components that is a direct copy/paste from the description in the System Security Plan.

This <Information System Name> that is undergoing testing as described in this Security Assessment Plan is named in Table 2-1.

Unique Identifier	Information System Name	Information System Abbreviation

Table 2-1 – Information System Name and Title

The physical locations of all the different components that will be tested are described in Table 2-2.

Data Center Site Name	Address	Description of Components

Table 2-2 – Location of Components

See Previous Section for "Information System Name and Title"

Information in the SSP is cited from the SAP using its ID. See *Section 3.5, Importing the System Security Plan* for more information.

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling.
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. SAP Location of Components

The SAP references location information in the SSP using its ID, and must explicitly cite each location within the scope of the assessment. While `all` is valid OSCAL syntax, FedRAMP requires locations to be explicitly cited, so that the assessor can add their own description of the location. Also, the SSP will likely also contain locations that are not data centers.

Representation

```
<assessment-subject type="location">
   <description>
      <p>A description of the locations.</p>
   </description>
   <include-subject subject-uuid="uuid-of-location-in-SSP-metadata">
      <remarks>
         <p>Briefly describe the components at this location.</p>
      </remarks>
   </include-subject>
   <include-subject subject-uuid="uuid-of-location-in-SAP-metadata">
      <remarks>
         <p>Briefly describe the components at this location.</p>
      </remarks>
   </include-subject>
</assessment-subject>
```

XPath Queries

```
(SSP) List the Data Center UUIDs in the SSP (Primary and Alternate):
  /*/metadata/location[prop[@name='type'][@value='data-center']]/@uuid

(SSP) List the Primary Data Center UUIDs in the SSP:
  /*/metadata/location[prop[@name='type'][@value='data-center'][@class='primary']]/@uuid

NOTE: For just alternate data centers, replace 'primary' with 'alternate'.

(SAP) Location UUID (First Location cited in SAP):
  /*/assessment-subject[@type='location']/include-subject[1]/@subject-uuid

NOTE: Replace "[1]" with "[2]", "[3]", etc.

(SSP) Data Center Site Name (Lookup in SSP, using ID cited in SAP):
  /*/metadata/location[@id='location-2']/prop[@name='title']
  [@ns='https://fedramp.gov/ns/oscal']

NOTE: Replace 'location-2' with the SSP location as cited in the SAP.

(SSP or SAP) Address:
  /*/metadata/location[@uuid='uuid-value-from-SAP']/address/addr-line

NOTE: Replace addr-line with city, state, and postal-code as needed.
  There may be more than one addr-line.

NOTE: Replace 'location-2' with the SSP location as cited in the SAP.

(SSP) CSP's Description of Location (from SSP):
  /*/metadata/location[@uuid='uuid-value-for-location-2']/remarks

(SAP) Assessor's Description of Components at the first location:
  /*/assessment-subject[@type='location']/include-subject[1]/remarks/node()

NOTE: Replace "[1]" with "[2]", "[3]", etc.
```

4.3.1. If No OSCAL-based SSP Exists or Has Inaccurate Information (Locations)

If no OSCAL-based SSP exists, or the location of components is not accurately reflected in the SSP, this information may be added to the SAP's `metadata` section using the same syntax as the SSP. The `include-subject` citations are still required as described above; however, the IDs point to the SAP's location data instead of the SSP's.

The same queries work as presented above; however, the queries are used in the SAP instead of the SSP.

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

2.2. IP ADDRESSES SLATED FOR TESTING

Instruction: List the IP address of all systems that will be tested. Obtain this information from the System Security Plan and the CSP. Note that the IP addresses found in the System Security Plan must be consistent with the boundary. For a large network (Class B or larger), test a subset of the IP addresses. All scans must be fully authenticated. Add additional rows to the table as necessary. In lieu of filling out this table, CSPs may embed a separate file or refer to Appendix C, as long as all required information is included. In addition, CSPs may use any unique identifier (e.g. MAC address or hostname), instead of the IP address.

CSPs must ensure that the inventory is current before testing, and that the inventory and components to be tested are in agreement.

IP addresses and network ranges of the system that will be tested are noted in Table 2-3 or attached as an embedded Excel file in appendix C.

IP Address(s) or Ranges	Hostname	Software & Version	Function

Table 2-3 – Components Slated for Testing

FedRAMP Component vs. OSCAL Component

FedRAMP uses the term "component" to generally mean any component of a system, especially its system inventory. OSCAL distinctly separates "components" and "inventory-items", while maintaining a relationship between the two. From FedRAMP's perspective, an inventory-item is still a component. This distinction becomes important when representing FedRAMP "components" in OSCAL.

The [1] indicates the first `uuid-ref` within any `include-subject` of type "inventory-item".

4.4. SAP IP Addresses Slated for Testing

The SAP references SSP content for this information. Each subnet should be represented in the SSP as a `component`, with `type='subnet'`. If the SSP does not enumerate subnets in this way, the SAP tool should allow the assessor to add them to the SAP's `local-definitions` as components.

Beyond subnets, this section is an enumeration of the SSP's `inventory-item` assemblies, which always contain the hostname and IP address of the item. Other details, such as the software and version information, may be found in the inventory item itself or the SSP inventory item may be linked to an SSP component containing those details, depending on whether the SSP is using the legacy (flat) approach or the preferred component approach.

If the assessor needs to add missing component or inventory-item entries, or if the assessor needs to correct this information, the SAP tool must add this assessor-provided information to the SAP's local-definitions.

See the *Guide to OSCAL-based FedRAMP System Security Plans* to learn more about legacy (flat-file) and component-based inventory approaches. Use a combination of `include-subject` and `exclude-subject` assemblies to specify the SSP IDs of all in-scope components and inventory-items. Excluding items is typically used in association with the rules of engagement.

If an inventory-item is linked to a component in the SSP, the component is automatically within scope, as this is often necessary to get the software and version information. Tools should honor this relationship and consider linked components to be implicitly in-scope, even if the component was not explicitly cited in the SAP.

Representation

```
<assessment-subject type="component">
   <description><p>A description of the included component.</p></description>
   <include-all />
   <exclude-subject subject-uuid="uuid-of-SSP-component-to-exclude" />
</assessment-subject>

<assessment-subject type="inventory-item">
   <description><p>Description of the included inventory.</p></description>
   <include-all />
   <exclude-subject subject-uuid="uuid-of-SSP-inventory-item-to-exclude" />
   <exclude-subject subject-uuid="uuid-of-SSP-inventory-item-to-exclude" />
</assessment-subject>
<!-- OR -->
<assessment-subject type="inventory-item">
   <description><p>Description of the included inventory.</p></description>
   <include-subject subject-uuid="uuid-of-SSP-inventory-item-to-include" />
   <include-subject subject-uuid="uuid-of-SSP-inventory-item-to-include" />
   <exclude-subject subject-uuid="uuid-of-SSP-inventory-item-to-exclude" />
</assessment-subject>
```

XPath Queries

```
(SAP) Should all inventory-items be included? (true/false):
  boolean(/*/assessment-subject[@type='inventory-item']/include-all)

NOTE: This means all inventory-items in the SSP's system-implementation as well as all
  inventory-items in the SAP's local definitions

(SAP) Get the first inventory-item UUID from the SAP:
  /*/assessment-subject[@type='inventory-item']/include-subject[1]/@subject-uuid

(SSP) Get Host Name from inventory-item in the SSP:
  /*/system-implementation/system-inventory/
  inventory-item[@uuid='uuid-value-from-above']/prop[@name='fqdn']
```

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

2.2. IP ADDRESSES SLATED FOR TESTING

Instruction: List the IP address of all systems that will be tested. Obtain this information from the System Security Plan and the CSP. Note that the IP addresses found in the System Security Plan must be consistent with the boundary. For a large network (Class B or larger), test a subset of the IP addresses. All scans must be fully authenticated. Add additional rows to the table as necessary. In lieu of filling out this table, CSPs may embed a separate file or refer to Appendix C, as long as all required information is included. In addition, CSPs may use any unique identifier (e.g. MAC address or hostname), instead of the IP address.

CSPs must ensure that the inventory is current before testing, and that the inventory and components to be tested are in agreement.

IP addresses and network ranges of the system that will be tested are noted in Table 2-3 or attached as an embedded Excel file in appendix C.

IP Address(s) or Ranges	Hostname	Software & Version	Function

Table 2-3 – Components Slated for Testing

4.4.1. If No OSCAL-based SSP Exists or Has Inaccurate Information (IP Addresses)

If no OSCAL-based SSP exists, or the inventory information is not accurately reflected in the SSP, this information may be added to the SAP's `local-definition` section as described below. The `include-subject` citations are still required as described above; however, the UUIDs point to the SAP's local definitions instead of the SSP.

Representation

```
<local-definitions>
   <inventory-item uuid="uuid-value">
      <description>
         <p>A Windows laptop, not defined in the SSP inventory.</p>
      </description>
      <prop name="ipv4-address" value=”10.1.1.99”/>
      <prop name="virtual" value=”no”/>
      <prop name="public" value=”no”/>
      <prop name="fqdn" value=”dns.name”/>
      <prop name="mac-address" value=”00:00:00:00:00:00”/>
      <prop name="software-name" value=”Windows 10”/>
      <prop name="version" value=”V 0.0.0”/>
      <prop name="asset-type" value=”os”/>
      <!-- Use any needed prop allowed in an SSP inventory item  -->
   </inventory-item>

   <inventory-item uuid="uuid-value" asset-id="none">
      <description><p>A subnet not defined in the SSP inventory.</p></description>
      <prop name="ipv4-subnet">10.20.30.0/24</prop>
      <!-- Use any needed prop allowed in an SSP inventory item  -->
   </inventory-item>
</local-definitions>

<assessment-subject type="inventory-item">
   <description><p>Description of the included inventory.</p></description>
   <include-subject subject-uuid="uuid-of-SAP-inventory-item-to-include" />
   <exclude-subject subject-uuid="uuid-of-SAP-inventory-item-to-include" />
</assessment-subject>
```

XPath Queries

```
(SAP) Get the included ID the same way:
  /*/assessment-subject[@type='inventory-item']/include-subject[2]/@subject-uuid

(SAP) Get Subnet from inventory-item in the SAP:
  /*/local-definitions/inventory-item[@uuid='value-from-above']/prop[@name='ipv4-
  subnet']/@value
```

<*CSP*> *FedRAMP Annual SAP Template* <*Date of modification*>

2.3. WEB APPLICATIONS SLATED FOR TESTING

Instruction: Insert any URLs and the associated login IDs that will be used for testing. Only list the login URL. Do not list every URL that is inside the login in the below table. In the Function column, indicate the purpose that the web-facing application plays for the system (e.g. control panel to build virtual machines). In lieu of filling out this table, CSPs may embed a separate file or refer to appendix C, as long as all required information is included. In addition, CSPs may use any unique identifier (e.g. MAC address or hostname), instead of the IP address.

Activities employed to perform role testing on web applications may include capturing POST and GET requests for each function. The various web based applications that make up the system, and the logins and their associated roles that will be used for testing are noted by URL in Table 2-4 or attached as an embedded Excel file in appendix C.

Login URL	Login ID	IP Address of Login Host	Function

Table 2-4 – Application URLs Slated for Testing

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling.
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. SAP Web Applications Slated for Testing

The SSP inventory data should already indicate which assets have a web interface, with the following FedRAMP extension:

```
<prop name="scan-type" ns="https://fedramp.gov/ns/oscal" value="web"/>
```

This typically appears in the `inventory-item` itself with the legacy approach, and appears in a `component` associated with the `inventory-item` if the SSP is using the component-based approach. See the *Guide to OSCAL-based System Security Plans (SSP)* for details on the flat-file and component-based approaches.

FedRAMP expects the assessor to review and validate the list of identified web applications, both initially in the SAP and as a result of the discovery scans once the assessment begins. SAP tools should facilitate this review and adjustment of inventory data as needed for the assessor to properly identify all web applications for testing.

For every web interface to be tested, whether pre-identified in the SSP inventory or identified by the assessor, there must be a `task` entry. If the inventory-item already contains the `login-url`, the tool should duplicate it here. If not, the tool should enable the assessor to add it here. A SAP tool should also enable the assessor to add a `login-id` for test users here. Both use FedRAMP Extensions.

Representation

```
<local-definitions>
   <activity uuid="uuid-value">
      <title>Web Application Test #1</title>
      <description><p>Describe this web application test.</p></description>
      <prop name="type" value="web-application"/>
   </activity>
</local-definitions>
<!-- cut: terms-and-conditions, reviewed-controls, assessment-subject -->
<task uuid="uuid-value">
   <title>Web Application Tests</title>
   <task uuid="uuid-value">
      <title>Web Application Test #1</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal" value="web-application"/>
      <prop name="login-url" ns="https://fedramp.gov/ns/oscal"
                                    value="https://service.offering.com/login"/>
      <prop name="login-id" ns="https://fedramp.gov/ns/oscal" value="test-user"/>
      <assessment-subject type="inventory-item">
         <include-subject subject-uuid="uuid-of-SSP-inventory-item" >
      <related-activity activity-uuid="uuid-of-web-application-activity" />
   </task>
</task>
```

XPath Queries

```
(SAP) Login URL:
  (/*//task[prop[@name='type'][@ns="https://fedramp.gov/ns/oscal"][@value='web-
  application']])[1]/prop[@name='login-url'][@ns="https://fedramp.gov/ns/oscal"]

(SAP) Login ID:
  (/*//task[prop[@name='type'][@ns="https://fedramp.gov/ns/oscal"][@value='web-
  application']])[1]/prop[@name='login-id'][@ns="https://fedramp.gov/ns/oscal"]

(SAP) Inventory-ID of host:
  (/*//task[prop[@name='type'][@ns="https://fedramp.gov/ns/oscal"][@value='web-
  application']])[2]/subject[@type='inventory-item']/include-subject/@subject-uuid

NOTE: Replace "[2]" with "[2]", "[3]", etc.

REMEMBER: The inventory-item could be in the SSP's system-implementation or the SAP's
  local-definitions.
```

2.4. DATABASES SLATED FOR TESTING

Instruction: Insert the hostnames, IP address, and any relevant additional information on the databases that will be tested. All scans must be fully authenticated. Add additional rows as necessary. In lieu of filling out this table, CSPs may embed a separate file or refer to appendix C, as long as all required information is included. In addition, CSPs may use any unique identifier (e.g. MAC address or hostname), instead of the IP address.

Databases that are slated for testing includes those listed in Table 2-5 or attached as an embedded Excel file in appendix B.

Database Name	Hostname	IP Address	Additional Info

Table 2-5 – Databases Slated for Testing

4.6. SAP Databases Slated for Testing

The SSP inventory data should already indicate which assets are a database, with the following FedRAMP extension:

```
<prop name="scan-type" ns="https://fedramp.gov/ns/oscal" value="database"/>
```

This typically appears in the `inventory-item` itself with the legacy (flat-file) approach and appears in a `component` associated with the `inventory-item` if the SSP is using the component-based approach. See the *Guide to OSCAL-based System Security Plans (SSP)* for details on the flat-file and component-based approaches.

FedRAMP expects the assessor to review and validate the list of identified databases, both initially in the SAP and as a result of discovery scans once the assessment begins. SAP tools should facilitate this review and adjustment of inventory data as needed for the assessor to properly identify all databases for testing.

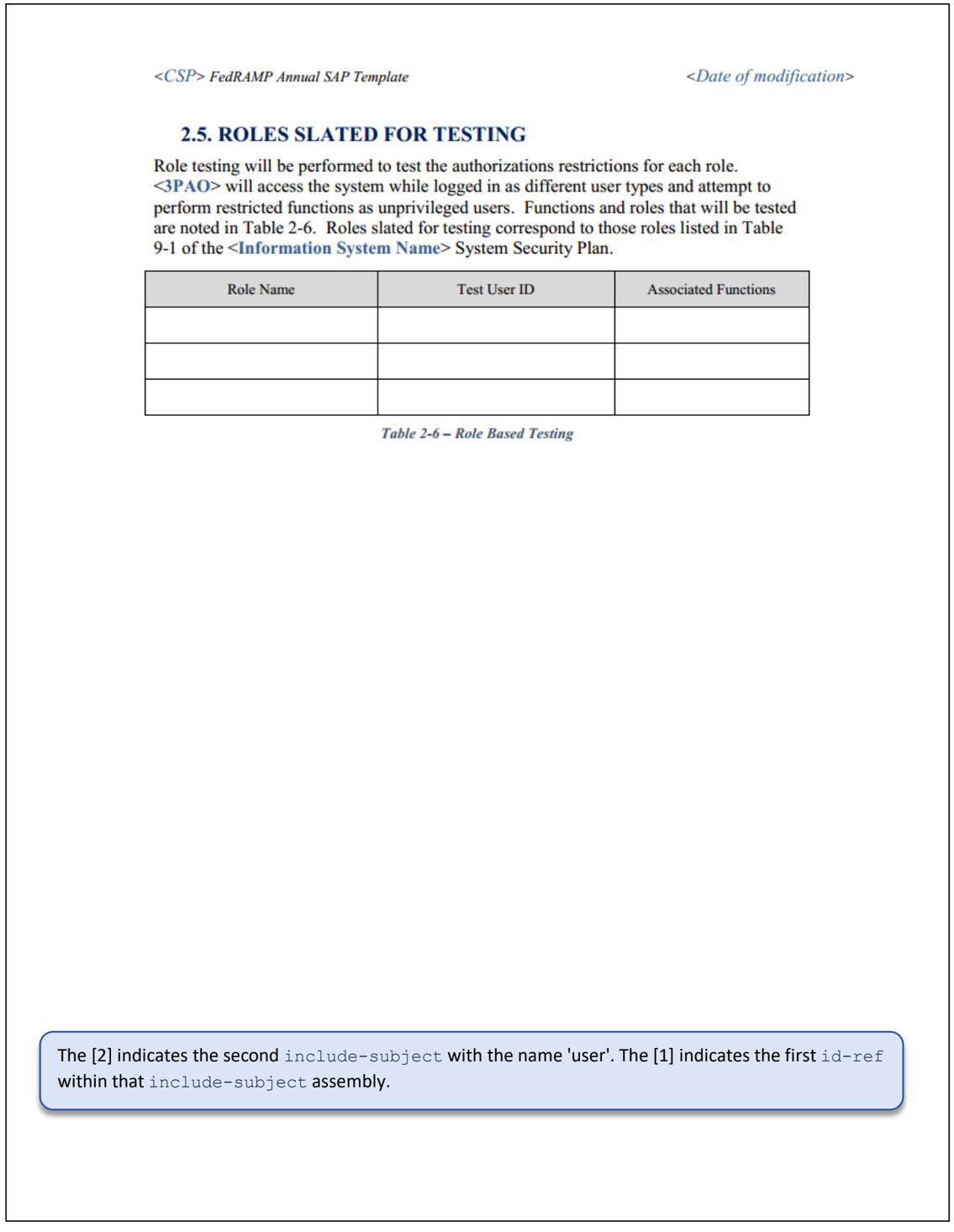
XPath Queries

```
(SSP) Host name of first database in SSP(flat file approach):
  (/*/system-implementation/system-inventory/inventory-item/prop[@name='scan-
  type'][string()='database'])[1]/../prop[@name='fqdn']

(SSP) Host name of the first database in SSP (component approach) [xPath 2.0+ only]:
  (let $key:=/*/system-implementation/component[prop [@name='scan-type']
  [@ns='https://fedramp.gov/ns/oscal']='database']/@id return /*/system-
  implementation/system-inventory/inventory-item [implemented-component/@component-
  id=$key]/prop[@name='fqdn'])[1]
```

4.6.1. If No OSCAL-based SSP Exists or Has Inaccurate Information (Database)

If no OSCAL-based SSP exists, or an item is missing completely from the SSP inventory, it should have already been added as described in *Section 4.4.1, If No OSCAL-based SSP Exists or Has Inaccurate Information (IP* Addresses).

If a pre-existing SSP inventory item fails to properly identify a database, the tool should enable the assessor to add this designation with an entry in the SAP `local-definitions`, except the value `database` should be used instead of `web` for the scan-type.



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

2.5. ROLES SLATED FOR TESTING

Role testing will be performed to test the authorizations restrictions for each role. <3PAO> will access the system while logged in as different user types and attempt to perform restricted functions as unprivileged users. Functions and roles that will be tested are noted in Table 2-6. Roles slated for testing correspond to those roles listed in Table 9-1 of the <Information System Name> System Security Plan.

Role Name	Test User ID	Associated Functions

Table 2-6 – Role Based Testing

The [2] indicates the second `include-subject` with the name 'user'. The [1] indicates the first `id-ref` within that `include-subject` assembly.

4.7. SAP Roles Slated for Testing

FedRAMP uses the term "roles"; however, in OSCAL syntax, these are "users". Under OSCAL, "roles" are something different. This distinction is subtle, yet important for tool development.

As with locations and inventory-items, if the "roles" slated for testing exist accurately in the SSP, they are referenced from the SAP using their IDs as they are assigned to `user` assemblies in the `system-implementation` section of the OSCAL-based SSP file.

Historically, FedRAMP assessors often identify more generic roles for testing than are enumerated in the SSP, such as "internal", "external", and "privileged". SAP tools should present assessors with the roles from the SSP so the assessor can select specific roles for testing. If the assessor elects to reference more generic roles, the SAP tool should enable the assessor to create these generic roles the same as if the roles were missing from the SSP.

Representation

```
<assessment-subject type="user">
   <description>
      <p>A description of the included roles.</p>
      <p>A description of an excluded role.</p>
   </description>
   <include-subject subject-uuid="uuid-from-SSP" />
   <exclude-subject subject-uuid="uuid-from-SSP" />
<assessment-subject>
```

For every role to be tested, whether pre-identified in the SSP inventory or identified by the assessor, there must be a `test-method` entry in the `assessment-activities` section. A SAP tool should enable the assessor to add a test user ID here.

See the next page for the representation of *Test User IDs*, as well as XPath Queries.

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

2.5. ROLES SLATED FOR TESTING

Role testing will be performed to test the authorizations restrictions for each role. <3PAO> will access the system while logged in as different user types and attempt to perform restricted functions as unprivileged users. Functions and roles that will be tested are noted in Table 2-6. Roles slated for testing correspond to those roles listed in Table 9-1 of the <Information System Name> System Security Plan.

Role Name	Test User ID	Associated Functions

Table 2-6 – Role Based Testing

As with locations and inventory-items, if the "roles" slated for testing exist accurately in the SSP, they are referenced from the SAP using their SSP IDs. These IDs reference `user` assemblies in the `system-implementation` section of the OSCAL-based SSP file.

Historically, FedRAMP assessors often identified generalized roles for testing, such as "internal", "external", and "privileged", rather than citing the specific roles enumerated in the SSP. This is in response to a FedRAMP requirement to test roles from each perspective.

Assessors are encouraged to identify roles in an OSCAL SAP more specifically. SAP tools should present assessors with the roles from the SSP so the assessor can select specific roles for testing. Assessors should ensure the selection of at least one role from each of the above generalized role categories. If the assessor elects to reference more generic roles, the SAP tool should enable the assessor to create these generic roles the same as if the roles were missing from the SSP. See the next section for more information.

Representation

```
<task uuid="EDDBCFA9-D296-4818-ADCC-3D5465ED3FDD" type="action">
   <title>Role-Based Tests</title>
   <task uuid="CFCB0F24-2E1B-49D7-B938-5F58479ED874" type="action">
      <title>Role Based Test #1</title>
      <prop name="test-type" ns="https://fedramp.gov/ns/oscal" vaule="role-based"/>
      <prop name="login-id" ns="https://fedramp.gov/ns/oscal" value="test-user"/>
      <prop                  name="user-uuid"                  ns="https://fedramp.gov/ns/oscal"
                                                  value="9cb0fab0-78bd-44ba-bcb8-3e9801cc952f"/>
      <associated-activity activity-uuid="dc858ece-b430-485d-886c-3a812bb77b13" />
   </task>
   <task uuid="74830d19-2820-4487-bd1d-91d8656b7eb0" type="action">
      <title>Role Based Test #2</title>
      <prop name="test-type" ns="https://fedramp.gov/ns/oscal" value="role-based"/>
      <prop name="login-id" ns="https://fedramp.gov/ns/oscal" value="test-admin"/>
      <prop                  name="user-uuid"                  ns="https://fedramp.gov/ns/oscal"
                                                  value="9cb0fab0-78bd-44ba-bcb8-3e9801cc952f"/>
      <associated-activity activity-uuid="64142a6f-d8d4-47c6-8bb1-a0e33f17664d" />
   </task>
</task>
```

.

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

3. ASSUMPTIONS

Instruction: The assumptions listed are default assumptions. The IA must edit these assumptions as necessary for each unique engagement.

The following assumptions were used when developing this Security Assessment Plan:

- <CSP> resources, including documentation and individuals with knowledge of the <CSP> systems and infrastructure and their contact information, will be available to <3PAO> staff during the time necessary to complete assessments.
- The <CSP> will provide login account information / credentials necessary for <3PAO> to use its testing devices to perform authenticated scans of devices and applications.
- The <CSP> will permit <3PAO> to connect its testing laptops to the <CSP> networks defined within the scope of this assessment.
- The <CSP > will permit communication from <3PAO> testing appliances to an internet hosted vulnerability management service to permit the analysis of vulnerability data.
- Security controls that have been identified as "Not Applicable" (e.g. AC-18 wireless access) in the System Security Plan will be verified as such and further testing will not be performed on these security controls.
- Significant upgrades or changes to the infrastructure and components of the system undergoing testing will not be performed during the security assessment period.
- For onsite control assessment, <CSP> personnel will be available should the <3PAO> staff determine that either after hours work, or weekend work, is necessary to support the security assessment.

The `part` assembly includes *Markup multiline*, which enables the text to be formatted. This requires special handling.
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

4.8. SAP Assumptions

SAP Assumptions use syntax similar to OSCAL control catalog statements. They have a sort-id, which a tool can use to ensure the intended sequence is maintained.

Representation

```
<terms-and-conditions>
   <part name="assumptions">
      <part name="assumption">
         <prop name="sort-id" value="001"/>
         <p>[CSP Name] resources, ... complete assessments.</p>
      </part>
      <part name="assumption">
         <prop name="sort-id" value="002"/>
         <p>The [CSP Name] will provide ... of devices and applications.</p>
      </part>
      <part name="assumption">
         <prop name="sort-id" value="003"/>
         <p>The [CSP Name] will permit ... of this assessment.</p>
      </part>
      <part name="assumption">
         <prop name="sort-id" value="004"/>
         <p>The [CSP Name] will permit ... of vulnerability data.</p>
      </part>
      <part name="assumption">
         <prop name="sort-id" value="005"/>
         <p>Security controls that ... on these security controls.</p>
      </part>
      <part name="assumption">
         <prop name="sort-id" value="006"/>
         <p>Significant upgrades ... security assessment period.</p>
      </part>
      <part name="assumption">
         <prop name="sort-id" value="007"/>
         <p>For onsite control assessment, ...the security assessment.</p>
      </part>
   </part>
</terms-and-conditions>
```

XPath Queries

```
(SAP) Obtain Sort IDs, for sorting by the SAP tool:
  /*/terms-and-conditions/part[@name='assumptions']/
  part[@name='assumption']/prop[@name='sort-id']

(SAP) The first assumption statement:
  /*/terms-and-conditions/part[@name='assumptions']/
  part[@name='assumption']/prop[@name='sort-id'] [.='001']/../(* except prop)

NOTE: Replace '001' with '002', '003', etc. for each sort-id based on desired order.
```

NOTES:

- If the tool is using XPath 1.0 or 2.0, the tool must sort the results of the sort-id list, and then obtain the assumptions in the intended sequence. XPath 3.0 has a sort function, which can perform the sort for the tool
- OSCAL does not support the insertion of values within Markup Multiline at this time. The tool must either replace each "[CSP Name]" and "[3PAO Name]" with the appropriate value, or enable the assessor to manually make those changes. This feature may be added to future version of OSCAL.

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

4. METHODOLOGY

Instruction: FedRAMP provides a documented methodology to describe the process for testing the security controls. IAs may edit this section to add additional information. The IA must must review the SAR to gain a full understanding of the documentation requirements for recording assessment results.

<3PAO> will perform an assessment of the **<Information System Name>** security controls using the methodology described in NIST SP 800-53A. **<3PAO>** will use FedRAMP supplied test procedures to evaluate the security controls. Contained in Excel worksheets, these test procedures contain the test objectives and associated test cases to determine if a control is effectively implemented and operating as intended. The results of the testing shall be recorded in the worksheets (provided in Appendix B) along with information that notes whether the control (or control enhancement) is satisfied or not.

<3PAO> data gathering activities will consist of the following:

- Request **<CSP>** to provide FedRAMP required documentation
- Request any follow-up documentation, files, or information needed that is not provided in FedRAMP required documentation
- Travel to the CSP sites as necessary to inspect systems and meet with CSP staff
- Obtain information through the use of security testing tools

Security controls will be verified using one or more of the following assessment methods:

- Examine: the IA will review, analyze, inspect, or observe one or more assessment artifacts as specified in the attached test cases;
- Interview: the IA will conduct discussions with individuals within the organization to facilitate assessor understanding, achieve clarification, or obtain evidence;
- Technical Tests: the IA will perform technical tests, including penetration testing, on system components using automated and manual methods.

<3PAO> <will or will not> use sampling when performing this assessment.

Instruction: If sampling methodology is used, attach the sampling methodology in Appendix C.

Penetration testing methodology is attached in Appendix D.

The `part` assembly includes *Markup multiline,* which enables the text to be formatted. This requires special handling.
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

4.9. SAP Methodology

In general, the methodology is simply a single markup multiline field, which enables the assessor to modify the content using rich text formatting.

FedRAMP requires the presence of the `sampling` property, which indicates whether sampling will be used by the assessor for the assessment. CSP tools must display a definitive statement based on the value of this property as follows:

- If the `sampling` property is '`yes`' (case sensitive), the statement should say, "[3PAO Name] will use sampling when performing this assessment." The "[3PAO Name]" should be replaced with the actual name of the assessor.
- If the sampling property is '`no`' (case sensitive), the statement should say, "[3PAO Name] will not use sampling when performing this assessment." The "[3PAO Name]" should be replaced with the actual name of the assessor.
- If the sampling property contains any other value, or is missing, the SAP tool should raise an error.

Representation

```
<terms-and-conditions>
   <part name="methodology">
      <prop name='sampling' ns='https://fedramp.gov/ns/oscal' value='no'/>
      <p>[3PAO Name] will perform ... is satisfied or not.</p>
      <p>[3PAO Name] data gathering activities will consist of the following:</p>
      <ul>
         <li>Request [CSP Name] provide FedRAMP required documentation</li>
         <li>Request any follow-up ... required documentation</li>
         <li>Travel to the [CSP Name] sites ... with [CSP Name] staff</li>
         <li>Obtain information through the use of security testing tools</li>
      </ul>
      <p>Security controls will ... of the following assessment methods:</p>
      <ul>
         <li>Examine: the IA will ... the attached test cases</li>
         <li>Interview: the IA will ... clarification, or obtain evidence</li>
         <li>Technical Tests: the IA will perform ... manual methods</li>
      </ul>
   </part>
</terms-and-conditions>
```

FedRAMP Extension (Sampling Plans)
prop (`ns="https://fedramp.gov/ns/oscal"`):
- `name="sampling"`

XPath Queries

```
(SAP) Will the assessor use sampling?:
  /*/terms-and-conditions/part[@name='methodology']/prop[@name='sampling']/@value

(SAP) Methodology Description:
  /*/terms-and-conditions/part[@name='methodology']/(* except prop)
```

NOTES:

- The SAP tool should provide the assessor with an automated way to replace [CSP Name] and [3PAO Name] with the actual names of those parties.
- The SAP tool should allow the assessor to modify this content as needed.

<*CSP*> *FedRAMP Annual SAP Template* <*Date of modification*>

5. TEST PLAN

The schedule for testing, testing roles and the testing tools that will be used are described in the sections that follow.

5.1. SECURITY ASSESSMENT TEAM

Instruction: List the members of the risk assessment team and the role each member will play. Include team members contact information.

The security assessment team consists of individuals from **<3PAO >** which are located at **<Address of 3PAO>**. Information about **<3PAO >** can be found at the following URL: **<insert URL>**.

Security control assessors play a unique role in testing system security controls. NIST 800-39, *Managing Information Security Risk* states:

> *The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).*

The members of the IA security testing team are found in Table 5-1.

Name	Role	Contact Information

Table 5-1 – Security Testing Team

4.10. SAP Test Plan: Assessor's Name, Address, and URL

The SAP's metadata is used to represent the assessor's name address and URL. This uses the OSCAL common `role`, `party`, and `responsible-party` assemblies. Some `roles` are specific to the SAP. In the `responsible-party` assembly, the `party-uuid` may point to a party in the SSP or SAP. The SAP tool must not assign a role ID or party ID that duplicates one used in the SSP.

Representation

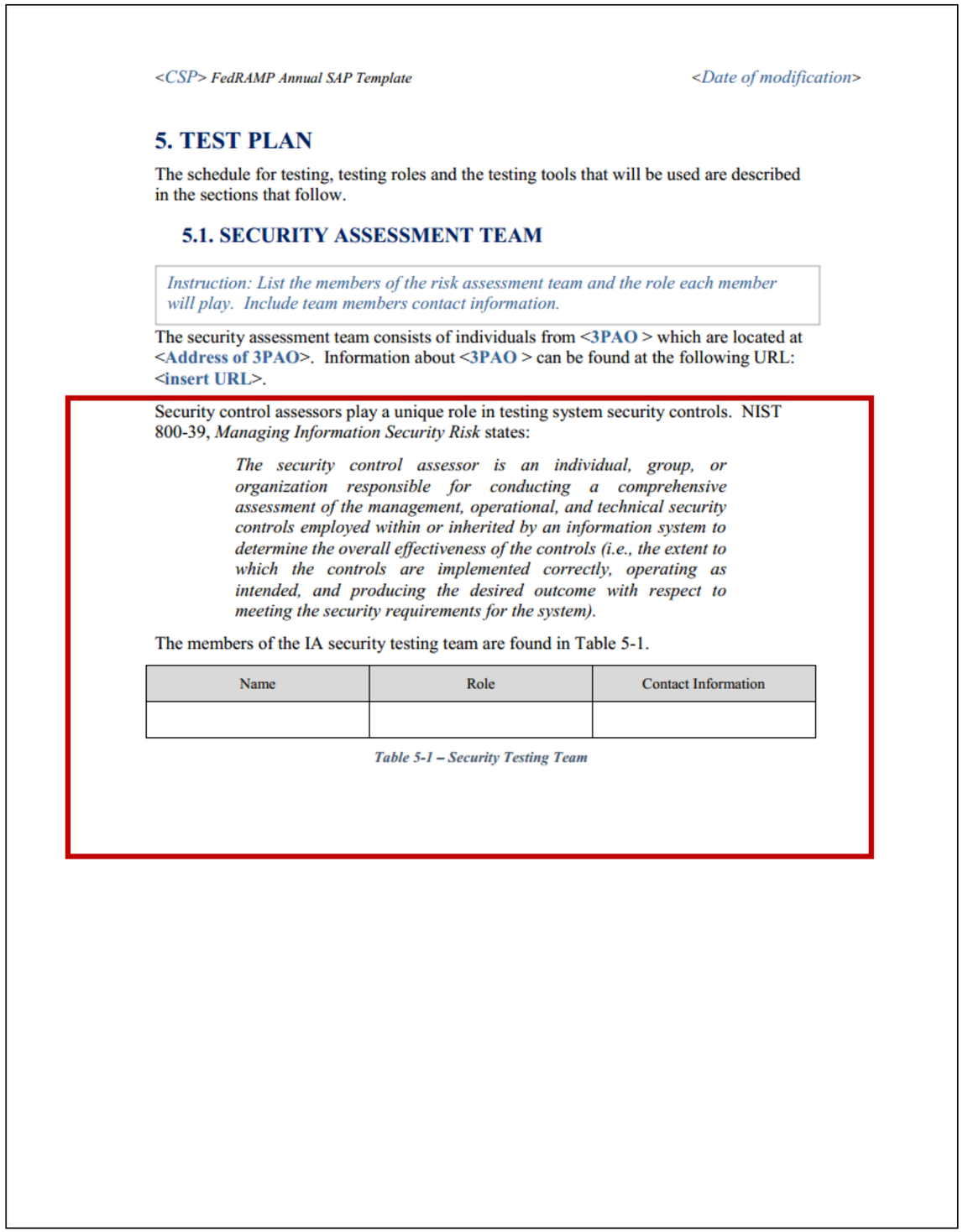
```
<metadata>
   <!-- cut: title, published, last-modified, version, oscal-version, prop -->
   <role id="assessor">
      <title>Assessment Organization</title>
      <desc>The organization performing the assessment.</desc>
   </role>
   <location uuid="uuid-value">
      <address type='work'>
         <addr-line>Suite 0000</addr-line>
         <addr-line>1234 Some Street</addr-line>
         <city>Haven</city>
         <state>ME</state>
         <postal-code>00000</postal-code>
         <country>US</country>
      </address>
   </location>
   <party uuid="uuid-value"  type="organization">
      <name>Assessment Organization Name</name>
      <short-name>Acronym/Short Name</short-name>
      <location-uuid>sap-location-1</location-id>
      <url>https://assesor.web.site</url>
      <prop name="iso-iec-17020-identifier"
                                        ns='https://fedramp.gov/ns/oscal'>0000.00</prop>
   </party>
   <responsible-party role-id="assessor">
      <party-uuid>uuid-of-assessor</party-uuid>
   </responsible-party>
</metadata>
```

FedRAMP Defined Identifier
role ID: `assessor`

FedRAMP Extension (A2LA Certification #)
prop (`ns="https://fedramp.gov/ns/oscal"`):
- `name="iso-iec-17020-identifier"`

XPath Queries

```
(SAP) Assessor's Name:
  /*/metadata/party[@id=(/*/metadata/responsible-party[@role-id='assessor']/party-uuid)]
  /org/org-name

(SAP) Assessor's Street Address (replace addr-line with city, state, etc.):
  /*/metadata/location[@id=/*/metadata/party[@id=(/*/metadata/responsible-party[@role-
  id='assessor']/party-uuid)]/org/location-id]/address/addr-line

(SAP) Assessor's Web Site:
  /*/metadata/party[@id=(/*/metadata/responsible-party[@role-id='assessor']/party-uuid)]
  /org/url

(SAP) 3PAO's A2LA Certification Number:
  /*/metadata/party[@id=(/*/metadata/responsible-party[@role-id='assessor']/party-uuid)]
  /org/prop[@name='iso-iec-17020-identifier'][@ns='https://fedramp.gov/ns/oscal']
```



<*CSP*> *FedRAMP Annual SAP Template* <*Date of modification*>

5. TEST PLAN

The schedule for testing, testing roles and the testing tools that will be used are described in the sections that follow.

5.1. SECURITY ASSESSMENT TEAM

Instruction: List the members of the risk assessment team and the role each member will play. Include team members contact information.

The security assessment team consists of individuals from **<3PAO >** which are located at **<Address of 3PAO>**. Information about **<3PAO >** can be found at the following URL: **<insert URL>**.

Security control assessors play a unique role in testing system security controls. NIST 800-39, *Managing Information Security Risk* states:

> *The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).*

The members of the IA security testing team are found in Table 5-1.

Name	Role	Contact Information

Table 5-1 – Security Testing Team

4.11. SAP Test Plan: Security Assessment Team

The SAP's metadata is used to represent the assessment team and assessment lead. This uses the OSCAL common `role`, `party`, and `responsible-party` assemblies. Some `roles` are specific to the SAP. The SAP tool must not assign a role ID or party ID that duplicates one used in the SSP.

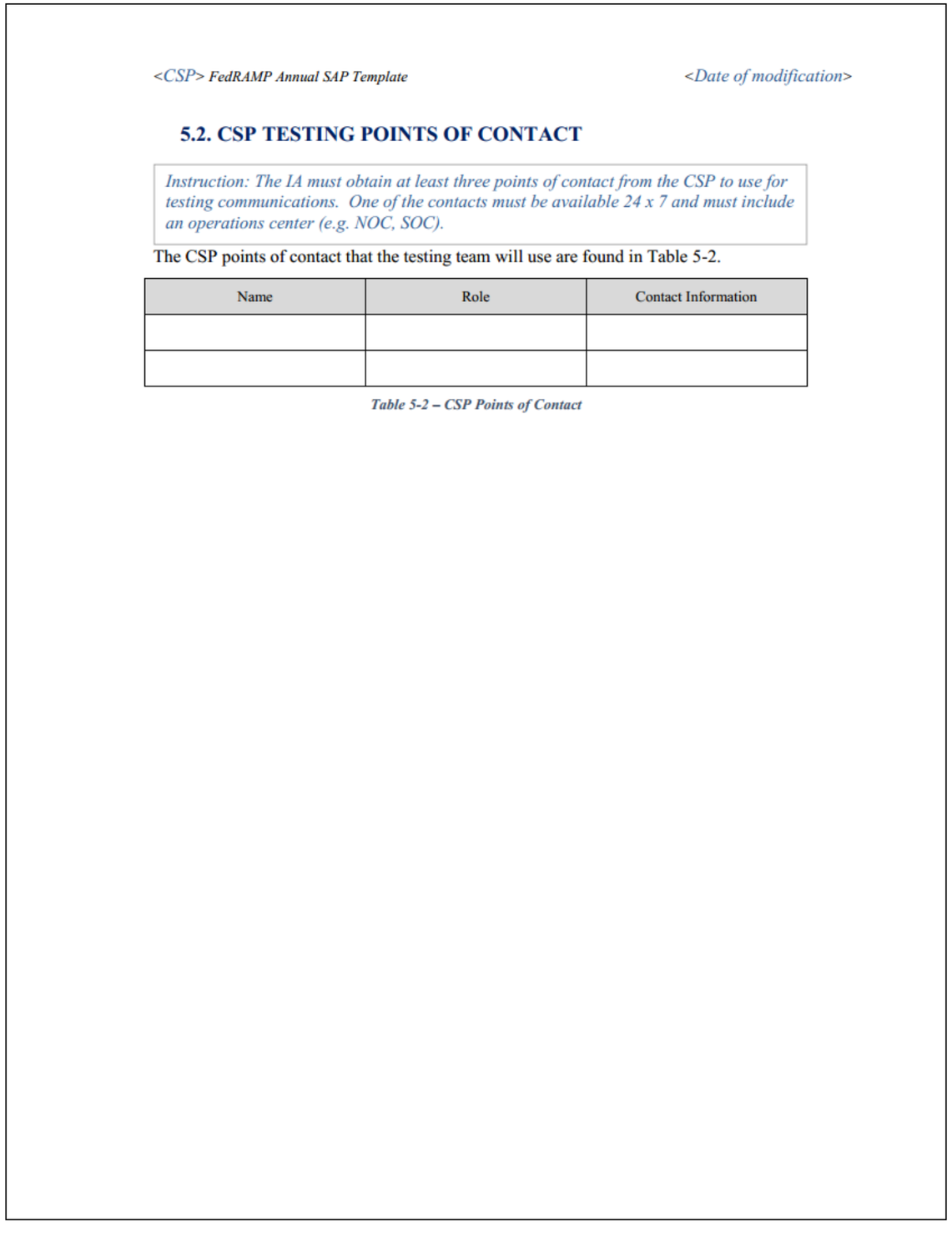
Representation

```
<metadata>
   <!-- cut: title, published, last-modified, version, oscal-version, prop -->
   <role id="assessment-team">
      <title>Assessment Team</title>
      <desc>The individual or individuals performing the assessment.</desc>
   </role>
   <party id="sap-person-2"  type="person">
      <person-name>[SAMPLE]Person Name 2</person-name>
      <org-id>assessment-org</org-id>
      <location-id>sap-location-1</location-id>
      <email>name@org.domain</email>
      <phone>202-000-0000</phone>
   </party>
   <!-- Repeat party for each person 3 - 5 -->
   <responsible-party role-id="assessment-team">
      <party-uuid>sap-person-2</party-uuid>
      <party-uuid>sap-person-3</party-uuid>
      <party-uuid>sap-person-4</party-uuid>
      <party-uuid>sap-person-5</party-uuid>
   </responsible-party>
</metadata>
```

FedRAMP Defined Identifier
role ID: `assessment-team`

XPath Queries

```
(SAP) Number of Assessment Team Members (integer):
  count(/*/metadata/responsible-party[@role-id='assessment-team']/party-uuid)

(SAP) Name of First Assessment Team Member:
  /*/metadata/party[@id=/*/metadata/responsible-party[@role-id='assessment-team']
  /party-uuid[1]]/person/person-name

(SAP) Role of First Assessment Team Member:
  /*/metadata/role[@id='assessment-team']/title

(SAP) Contact Information of First Assessment Team Member (phone):
  /*/metadata/party[@id=/*/metadata/responsible-party[@role-id='assessment-team']
  /party-uuid[1]]/person/phone

NOTE: Replace 'phone' with 'email'

NOTE: Replace [1] as needed with [2], [3], etc.
```



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

5.2. CSP TESTING POINTS OF CONTACT

Instruction: The IA must obtain at least three points of contact from the CSP to use for testing communications. One of the contacts must be available 24 x 7 and must include an operations center (e.g. NOC, SOC).

The CSP points of contact that the testing team will use are found in Table 5-2.

Name	Role	Contact Information

Table 5-2 – CSP Points of Contact

4.12. SAP Test Plan: CSP Testing Points of Contact

The SAP's metadata is used to represent the CSP's points of contact. This uses the OSCAL common `role`, `party`, and `responsible-party` assemblies. In the `responsible-party` assembly, the `party-uuid` may point to a party in the SSP or SAP. The SAP tool must not assign a role ID or party ID that duplicates one used in the SSP. If an individual is already identified via a party assembly in the SSP, that individual's information should not be duplicated in the SAP. Instead, the SAP should reference the SSP party ID for that individual.

Representation

```
<metadata>
   <role id="csp-assessment-poc">
      <title>CSP POCs During Testing</title>
      <desc>At least three CSP POCs must be identified in a FedRAMP SAP.</desc>
   </role>

   <!-- Only define a CSP party in the SAP when no appropriate party exits in SSP -->

   <responsible-party role-id="csp-assessment-poc">
      <!-- At least three -->
      <party-uuid>person-1</party-uuid>
      <party-uuid>person-2</party-uuid>
      <party-uuid>soc</party-uuid>
   </responsible-party>
</metadata>
```

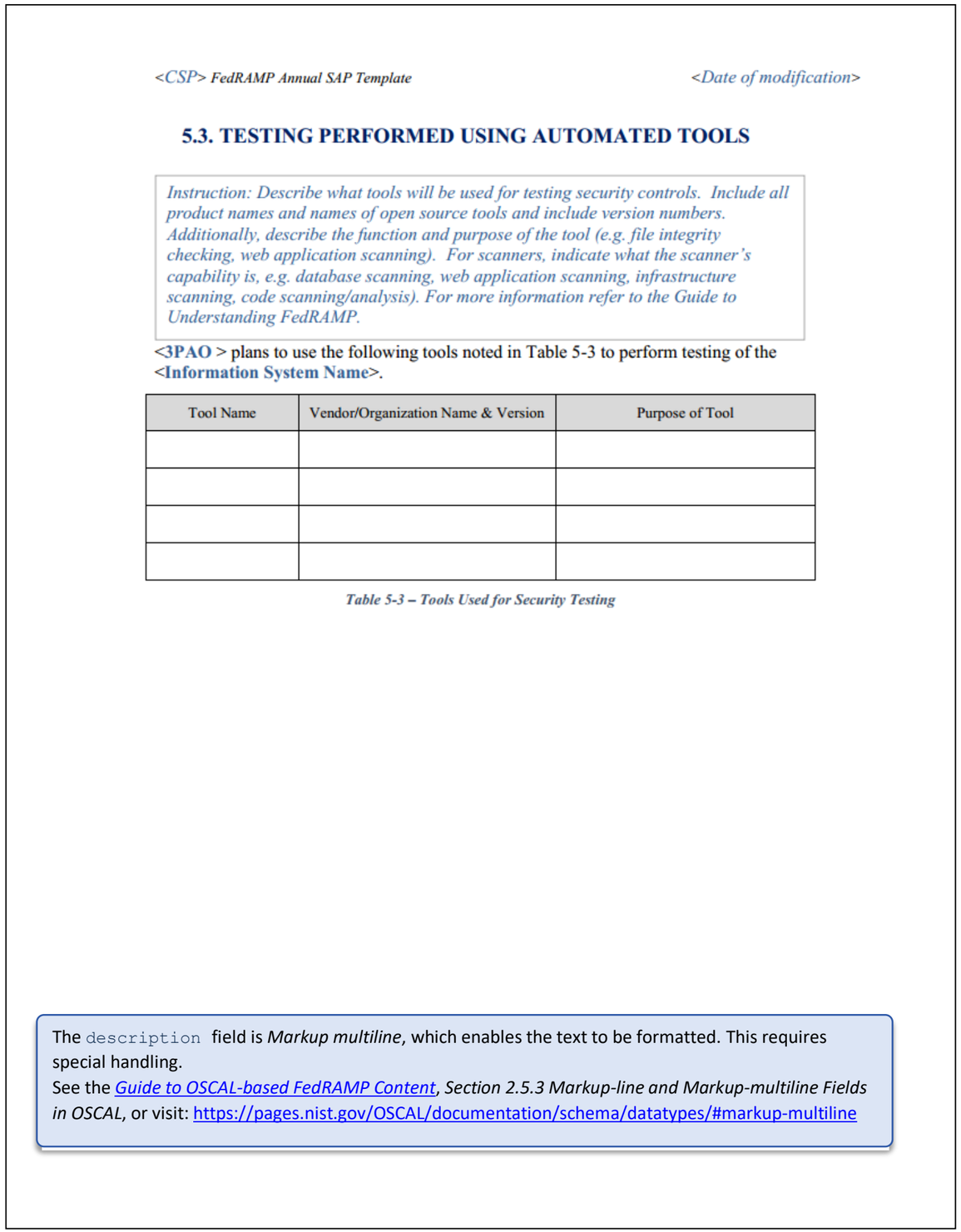
FedRAMP Defined Identifier
role ID: `csp-assessment-poc`

XPath Queries

```
(SAP) Number of CSP Assessment POCs (integer):
  count(/*/metadata/responsible-party[@role-id='csp-assessment-poc']/party-uuid)

(SAP) ID of the first CSP Assessment POC:
  /*/metadata/responsible-party[@role-id='csp-assessment-poc']/party-uuid[1]

NOTE: Replace [1] as needed with [2], [3], etc.

(SAP) Role:
  /*/metadata/role[@id='csp-assessment-poc']/title

(SSP) Name of the first person or organization:
  /*/metadata/party[@id='person-1']/(./person/person-name | ./org/org-name)

(SSP) Phone for the first person or organization:
  /*/metadata/party[@id='person-1']//phone

(SSP) Email for the first person or organization:
  /*/metadata/party[@id='person-1']//email

NOTE: Replace 'person-1' with each party-uuid found in the responsible role.
```

NOTES:

- IDs used for roles or parties in the SAP must not duplicate IDs used for roles or parties in the SSP.
- Only define a CSP party in the SAP when no appropriate party exists in the SSP.



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

5.3. TESTING PERFORMED USING AUTOMATED TOOLS

Instruction: Describe what tools will be used for testing security controls. Include all product names and names of open source tools and include version numbers. Additionally, describe the function and purpose of the tool (e.g. file integrity checking, web application scanning). For scanners, indicate what the scanner's capability is, e.g. database scanning, web application scanning, infrastructure scanning, code scanning/analysis). For more information refer to the Guide to Understanding FedRAMP.

<3PAO > plans to use the following tools noted in Table 5-3 to perform testing of the **<Information System Name>**.

Tool Name	Vendor/Organization Name & Version	Purpose of Tool

Table 5-3 – Tools Used for Security Testing

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling.
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

4.13. SAP Test Plan: Testing Performed Using Automated Tools

Automated tools are enumerated in the assets section of the SAP using the tools assembly. Each tool is listed using the same component syntax available in the SSP.

Representation

```
<assessment-assets >
   <component uuid="040937c3-2e0e-407a-bb3c-d4e61ac1c460" type="software">
      <title>XYZ Vulnerability Scanning Tool</title>
      <description>
         <p>Describe the purpose of the tool here.</p>
      </description>
      <prop name="vendor" value="Vendor Name"/>
      <prop name="name" value="Tool Name"/>
      <prop name="version" value="1.2.3"/>
      <status state="operational"/>
   </component>

   <component uuid="c50104b9-69b3-4383-a1f1-d8a6f6f806f7" type="software">
      <title>XYZ Database Scanning Tool</title>
      <description>
         <p>Describe the purpose of the tool here.</p>
      </description>
      <prop name="vendor" value="Vendor Name"/>
      <prop name="name" value="Tool Name"/>
      <prop name="version" value="1.2.3"/>
      <status state="operational"/>
   </component>
</assessment-assets >
   <!-- assessment-activities  -->
```

XPath Queries

```
(SAP) Number of Tools (integer):
  count(/*/assessment-assets/component)

(SAP) Name of first tool:
  /*/assessment-assets/component[1]/prop[@name='name']/@value

(SAP) Vendor/Organization Name of first tool:
  /*/assessment-assets/component[1]/prop[@name='vendor']/@value

(SAP) Version of first tool:
  /*/assessment-assets/component[1]/prop[@name='version']/@value

(SAP) Purpose of first tool:
  /*/assessment-assets/component[1]/description/node()

NOTE: Replace [1] as needed with [2], [3], etc.
```

NOTES:

- OSCAL syntax requires a `status` field within each `component` assembly. For assessment tools, the `state` should typically be '`operational`'.

<*CSP*> *FedRAMP Annual SAP Template* <*Date of modification*>

5.4. TESTING PERFORMED THROUGH MANUAL METHODS

Instruction: Describe what technical tests will be performed through manual methods without the use of automated tools. The results of all manual tests must be recorded in the SAR. Examples are listed in the first four rows. Delete the examples, and put in the real tests. Add additional rows as necessary. Identifiers must be in the format MT-1, MT-2 which would indicate "Manual Test 1" and "Manual Test 2" etc.

Test ID	Test Name	Description
MT-1	Forceful Browsing	We will login as a customer and try to see if we can gain access to the Network Administrator and Database Administrator privileges and authorizations by navigating to different views and manually forcing the browser to various URLs.
MT-3	CAPTCHA	We will test the CAPTCHA function on the web form manually.
MT-4	OCSP	We will manually test to see if OCSP is validating certificates.

Table 5-4 – Testing Performed Through Manual Methods

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling.
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

4.14. SAP Test Plan: Testing Performed Through Manual Methods

Representation

```
<local-definitions>
  <activity uuid="2715174e-9355-4775-bea4-4068e59e916b">
    <title>Title of the Manual Test</title>
    <description>
      <p>Description of the manual test</p>
    </description>
    <prop name="type" value="manual"/>
    <prop name="label" value="Test ID"/>
    <step uuid="fb039fd7-5a2b-4c0f-867c-88cce9c3778c ">
      <description><p>Describe test step #1</p></description>
      <prop name="sort-id" name="001"/>
    </step>
    <step uuid="fb039fd7-5a2b-4c0f-867c-88cce9c3778c ">
      <description><p>Describe test step #2</p></description>
      <prop name="sort-id" value="002"/>
    </step>
    <step uuid="fb039fd7-5a2b-4c0f-867c-88cce9c3778c ">
      <description><p>Describe test step #3</p></description>
      <prop name="sort-id">003</prop>
    </step>
  </activity>
  <activity uuid="3ba68918-80ef-4846-89e0-9f1def7e5223">
    <title>[SAMPLE]Forceful Browsing</title>
    <description>
      <p>We will login as a customer ...cut... browser to various URLs</p>
    </description>
    <prop name="type" value="manual"/>
    <prop name="label" value="Test ID"/>
  </activity>
</local-definitions>
```

XPath Queries

```
(SAP) Number of manual test methods (integer):
  count(/*/local-definitions/activity[prop[@name='type'][@value='manual']])

(SAP) Test ID of first manual test method:
  (/*/local-definitions/activity[prop[@name='type'][@value='manual']])
  [1]/prop[@name='label']

(SAP) Test Name of first manual test method:
  (/*/local-definitions/activity[prop[@name='type'][@value='manual']]) [1]/title

(SAP) Description of first manual test method:
  (/*/local-definitions/activity[prop[@name='type'][@value='manual']])
  [1]/description/node()

NOTE: Replace [1] as needed with [2], [3], etc.
```

NOTES:

- If a test method represents more than one test type, such as manual test that is also a role-based test, the `test-type` property should appear twice. Once indicating each type.

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

5.5. SCHEDULE

Instruction: Insert the security assessment testing schedule. This schedule must be presented to the CSP by the IA before commencing testing for Annual Assessment. The ISSO must be invited to the meeting that presents the schedule to the CSP. After being presented to the CSP, the IA must make any necessary updates to the schedule and this document and send an updated version to the CSP with a copy to the ISSO.

The security assessment testing schedule can be found in Table 5-5.

Task Name	Start Date	Finish Date
Prepare Test Plan		
Meeting to Review Test Plan		
Test Plan Update		
Review CSP Documentation		
Conduct Interviews of CSP Staff		
Perform Testing		
Vulnerability Analysis and Threat Assessment		
Risk Exposure Table Development		
Complete Draft SAR		
Draft SAR Delivered to SAP		
Issue Resolution Meeting		
Complete Final Version of SAR		
Send Final Version of SAR to CSP and ISSO		

Table 5-5 – Testing Schedule

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling.
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

4.15. SAP Test Plan: Schedule

Representation

```
<task uuid="17030aaf-7712-4228-8607-a5a97a785efa" type="action">
   <title>Prepare Test Plan</title>
   <description>
      <p>optional description here</p>
   </description>
   <timing>
      <within-date-range start="2020-06-01T00:00:00Z" end="2020-06-15T00:00:00Z"/>
   </timing>
</task>
<task uuid="b65e7779-bd3d-4a49-9de5-3122c290792f" type="action">
   <title>Meeting to Review Test Plan</title>
   <description>
      <p>optional description here</p>
   </description>
   <timing>
      <within-date-range start="2020-06-01T00:00:00Z" end="2020-06-15T00:00:00Z"/>
   </timing>
</task>
```

XPath Queries

```
(SAP) Number of tasks in schedule (integer):
  count(/*/task)

(SAP) Name of first task:
  /*/task[1]/title

(SAP) Start date of first task:
  /*/task[1]/timing/within-date-range/@start

(SAP) Finish date of first task:
  /*/task[1]/timing/within-date-range/@end

(SAP) Optional Description of first task:
  /*/task[1]/description/node()

NOTE: Replace [1] as needed with [2], [3], etc.
```

NOTES:

- In the OSCAL file, the start and end fields must use the OSCAL data type dateTime-with-timezone.
- The time may be entered as all zeros.
- For FedRAMP, a SAP tool should display only the date and ignore the time. The date should be presented to the user in a more user-friendly format.

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

6. RULES OF ENGAGEMENT

Instruction: FedRAMP provides and recommends the Rules of Engagement as listed in the section that follows. IAs must edit this ROE as necessary. The final version of the ROE must be signed by both the IA and CSP. See NIST SP 800-115, Appendix B for further guidance.

A Rules of Engagement (ROE) is a document designed to describe proper notifications and disclosures between the owner of a tested systems and an independent assessor. In particular, a ROE includes information about targets of automated scans and IP address origination information of automated scans (and other testing tools). Together with the information provided in preceding sections of this document, this document shall serve as a Rules of Engagement once signed.

6.1. DISCLOSURES

Instruction: Edit and modify the disclosures as necessary. If testing is to be conducted from an internal location, identify at least one network port with access to all subnets/segments to be tested. The purpose of identifying the IP addresses from where the security testing will be performed is so that when IAs are performing scans, the CSP will understand that the rapid and high volume network traffic is not an attack and is part of the testing.

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. All scans will originate from the following IP address(es): **<IP addresses>**

The `part` assembly includes *Markup multiline*, which enables the text to be formatted. This requires special handling.
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

4.16. SAP Rules of Engagement (ROE): Origination Addresses

The scan origination IP address(es) are included in the `assessment-platform` assembly. See the next page for other disclosures.

Representation

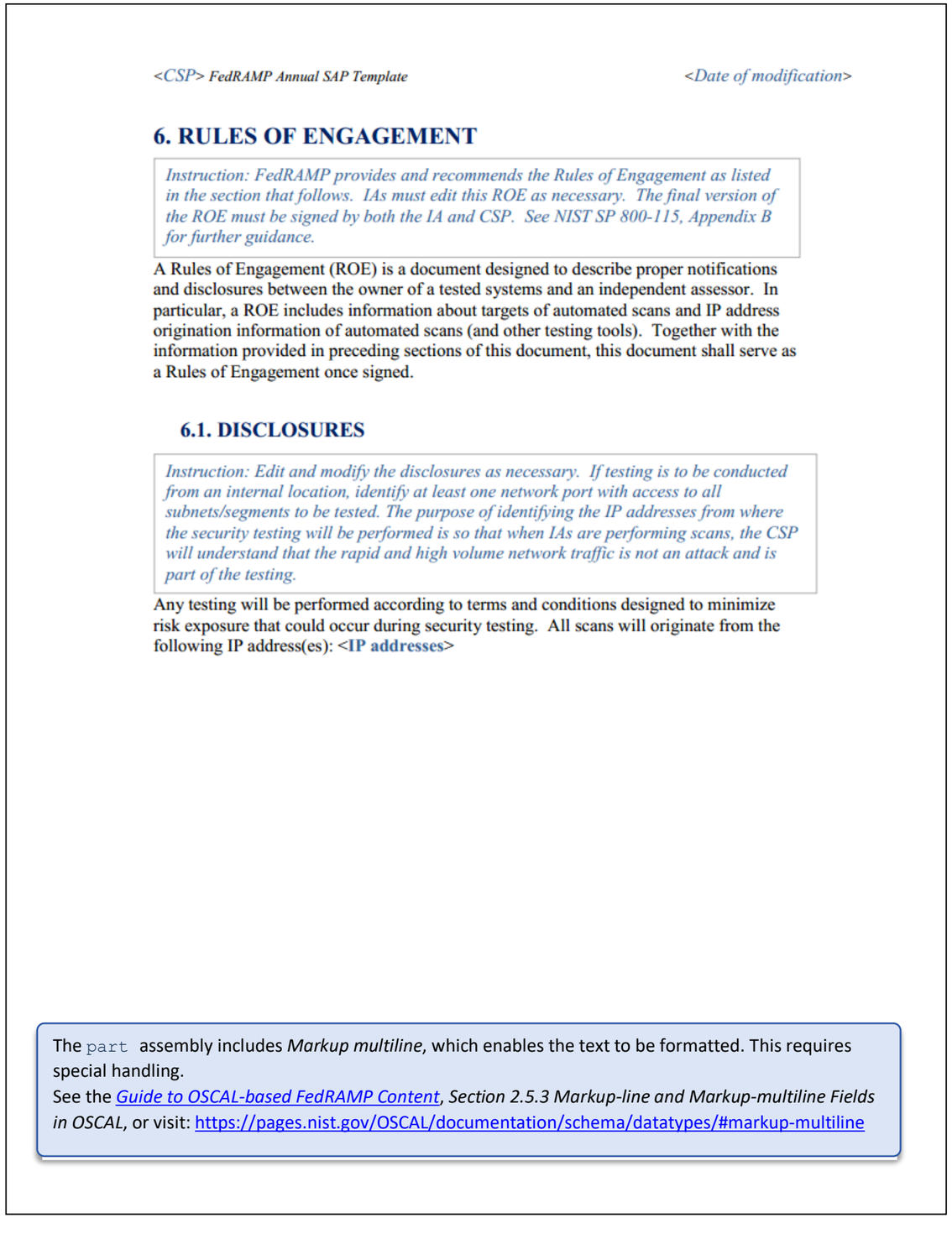
```
<assessment-assets>
   <component type="hardware" uuid="BA991C3F-1E00-4C38-BF81-86A9E503F3B9">
      <title>Assessment Laptop</title>
   </component>

   <component uuid="040937c3-2e0e-407a-bb3c-d4e61ac1c460" type="software">
      <title>XYZ Vulnerability Scanning Tool</title>
   </component>

   <component uuid="c50104b9-69b3-4383-a1f1-d8a6f6f806f7" type="software">
      <title>XYZ Database Scanning Tool</title>
   </component>

   <assessment-platform uuid="60218FE9-B01A-4553-B705-DBE9DEC44AA1">
      <title>Scanning Tools</title>
      <prop name="ipv4-address" value="10.10.10.10"/>
      <prop name="ipv4-address" value="10.10.10.11"/>
      <prop name="ipv4-address" value="10.10.10.12"/>
      <uses-component component-uuid="BA991C3F-1E00-4C38-BF81-86A9E503F3B9" >
         <remarks><p>Cites assessment laptop.</p></remarks>
      </uses-component>
      <uses-component component-uuid="BA991C3F-1E00-4C38-BF81-86A9E503F3B9">
         <remarks><p>Cites assessment laptop.</p></remarks>
      </uses-component>
      <uses-component component-uuid="040937c3-2e0e-407a-bb3c-d4e61ac1c460">
         <remarks><p>Cites Vulnerability Scanning Tool</p></remarks>
      </uses-component>
      <uses-component component-uuid="c50104b9-69b3-4383-a1f1-d8a6f6f806f7">
         <remarks><p>Cites Database Scanning Tool</p></remarks>
      </uses-component>
   </assessment-platform>
</assessment-assets>
```

XPath Queries

```
(SAP) Count scan origination addresses (integer):
  count(/*/assessment-assets/assessment-platform/prop[@name='ipv4-address'])

(SAP) First scan origination address:
  /*/assessment-assets/assessment-platform/prop[@name='ipv4-address'][1]

NOTE: Replace [1] as needed with [2], [3], etc.
```

NOTES:

- A SAP tool should present the scan origination addresses using the statement:
  "All scans will originate from the following IP address(es):", followed by the list of addresses.



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

6. RULES OF ENGAGEMENT

Instruction: FedRAMP provides and recommends the Rules of Engagement as listed in the section that follows. IAs must edit this ROE as necessary. The final version of the ROE must be signed by both the IA and CSP. See NIST SP 800-115, Appendix B for further guidance.

A Rules of Engagement (ROE) is a document designed to describe proper notifications and disclosures between the owner of a tested systems and an independent assessor. In particular, a ROE includes information about targets of automated scans and IP address origination information of automated scans (and other testing tools). Together with the information provided in preceding sections of this document, this document shall serve as a Rules of Engagement once signed.

6.1. DISCLOSURES

Instruction: Edit and modify the disclosures as necessary. If testing is to be conducted from an internal location, identify at least one network port with access to all subnets/segments to be tested. The purpose of identifying the IP addresses from where the security testing will be performed is so that when IAs are performing scans, the CSP will understand that the rapid and high volume network traffic is not an attack and is part of the testing.

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. All scans will originate from the following IP address(es): **<IP addresses>**

The `part` assembly includes *Markup multiline*, which enables the text to be formatted. This requires special handling.
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

4.17. SAP Rules of Engagement (ROE): Disclosures

The scan origination IP address(es) are included in the `assessment-platform` assembly. See the next page for other disclosures`.

Representation

```
<terms-and-conditions>
   <part name="disclosures">
      <part name="disclosure">
         <prop name="sort-id" value="001"/>
         <p>Any testing will be performed according to terms and conditions designed to
            Minimize risk exposure that could occur during security testing.</p>
      </part>
      <part name="disclosure">
         <prop name="sort-id" value="002"/>
         <p>A disclosure statement</p>
      </part>
   </part>
</terms-and-conditions>
```

XPath Queries

```
(SAP) Count other disclosure statements (integer):
  count(/*/terms-and-conditions/part[@name='disclosures']/part[@name='disclosure'])

(SAP) Obtain Sort IDs, for sorting by the SAP tool:
  /*/terms-and-
  conditions/part[@name='disclosures']/part[@name='disclosure']/prop[@name='sort-id']

(SAP) The first assumption statement:
  /*/terms-and-
  conditions/part[@name='disclosures']/part[@name='disclosure']/prop[@name='sort-id']
  [string()='001']/../(* except prop)

NOTE: Replace '001' with '002', '003', etc. for each sort-id based on desired order.
```

NOTES:

- A SAP tool should present the scan origination addresses using the statement:
  "All scans will originate from the following IP address(es):", followed by the list of addresses.

6.2. SECURITY TESTING MAY INCLUDE

Instruction: IAs must edit the bullets in this default list to make it consistent with each unique system tested.

Security testing may include the following activities:

- Port scans and other network service interaction and queries
- Network sniffing, traffic monitoring, traffic analysis, and host discovery
- Attempted logins or other use of systems, with any account name/password
- Attempted SQL injection and other forms of input parameter testing
- Use of exploit code for leveraging discovered vulnerabilities
- Password cracking via capture and scanning of authentication databases
- Spoofing or deceiving servers regarding network traffic
- Altering running system configuration except where denial of service would result
- Adding user accounts

4.18. SAP ROE: Security Testing May Include

Representation

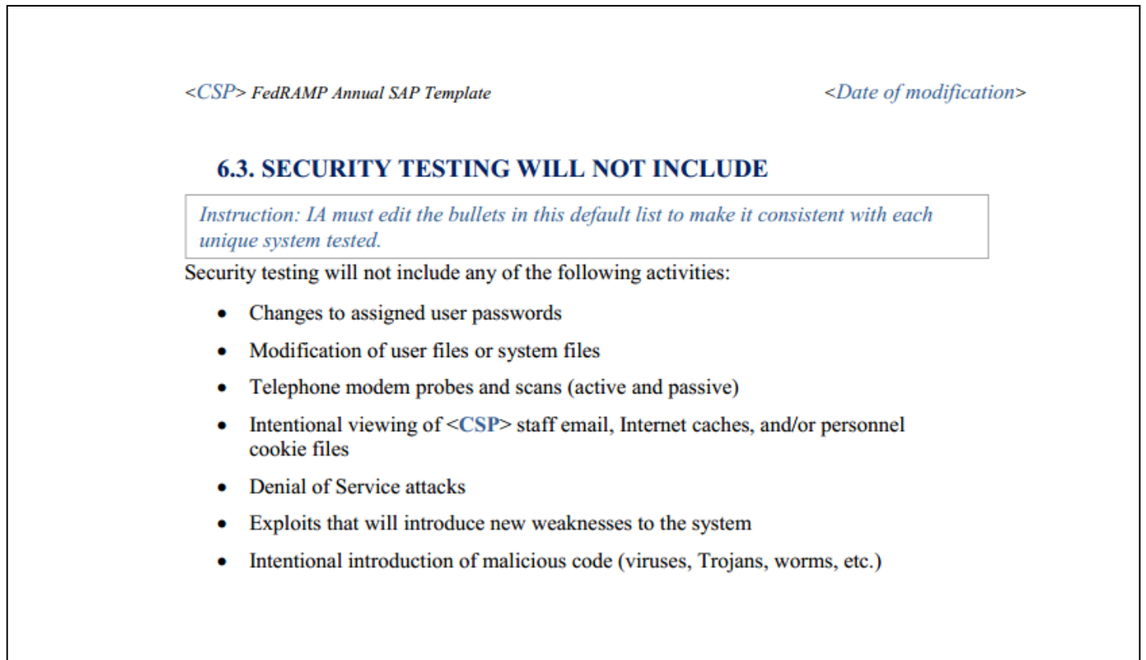
```
<terms-and-conditions>
   <part name="included-activities">
      <title>Included Activities</title>
      <p>The following activities are to be included as part of the FedRAMP assessment.</p>
      <part name="included-activity">

      </part>
      <part name="included-activity">
         <p>Port scans and other network service interaction and queries</p>
      </part>
      <part name="included-activity">
         <p>Network sniffing, traffic monitoring, traffic analysis, and host discovery</p>
      </part>
      <part name="included-activity">
         <p>Attempted logins or other use of systems, with any account name/password</p>
      </part>
      <part name="included-activity">
         <p>Attempted structured query language (SQL) injection and other forms of input
            parameter testing</p>
      </part>
      <part name="included-activity">
         <p>Use of exploit code for leveraging discovered vulnerabilities</p>
      </part>
      <part name="included-activity">
         <p>Password cracking via capture and scanning of authentication databases</p>
      </part>
      <part name="included-activity">
         <p>Spoofing or deceiving servers regarding network traffic</p>
      </part>
      <part name="included-activity">
         <p>Altering running system configuration except where denial of service would
result</p>
      </part>
      <part name="included-activity">
         <p>Adding user accounts</p>
      </part>
   </part>
<terms-and-conditions>
```

XPath Queries

```
(SAP) Number of Included Activities:
  count(/*/terms-and-conditions/part[@name='included-activities']/part[@name='included-
  activity'])

(SAP) First Included Activity:
  /*/terms-and-conditions/part[@name='included-activities']/part[@name='included-
  activity'][1]/node()

NOTE: Replace [1] as needed with [2], [3], etc.
```

NOTES:

- An assessment tool should present a list of included activities with a preceding phrase such as, "Security testing may include the following activities:"



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

6.3. SECURITY TESTING WILL NOT INCLUDE

Instruction: IA must edit the bullets in this default list to make it consistent with each unique system tested.

Security testing will not include any of the following activities:

- Changes to assigned user passwords
- Modification of user files or system files
- Telephone modem probes and scans (active and passive)
- Intentional viewing of <CSP> staff email, Internet caches, and/or personnel cookie files
- Denial of Service attacks
- Exploits that will introduce new weaknesses to the system
- Intentional introduction of malicious code (viruses, Trojans, worms, etc.)

4.19. SAP ROE: Security Testing Will Not Include

Representation

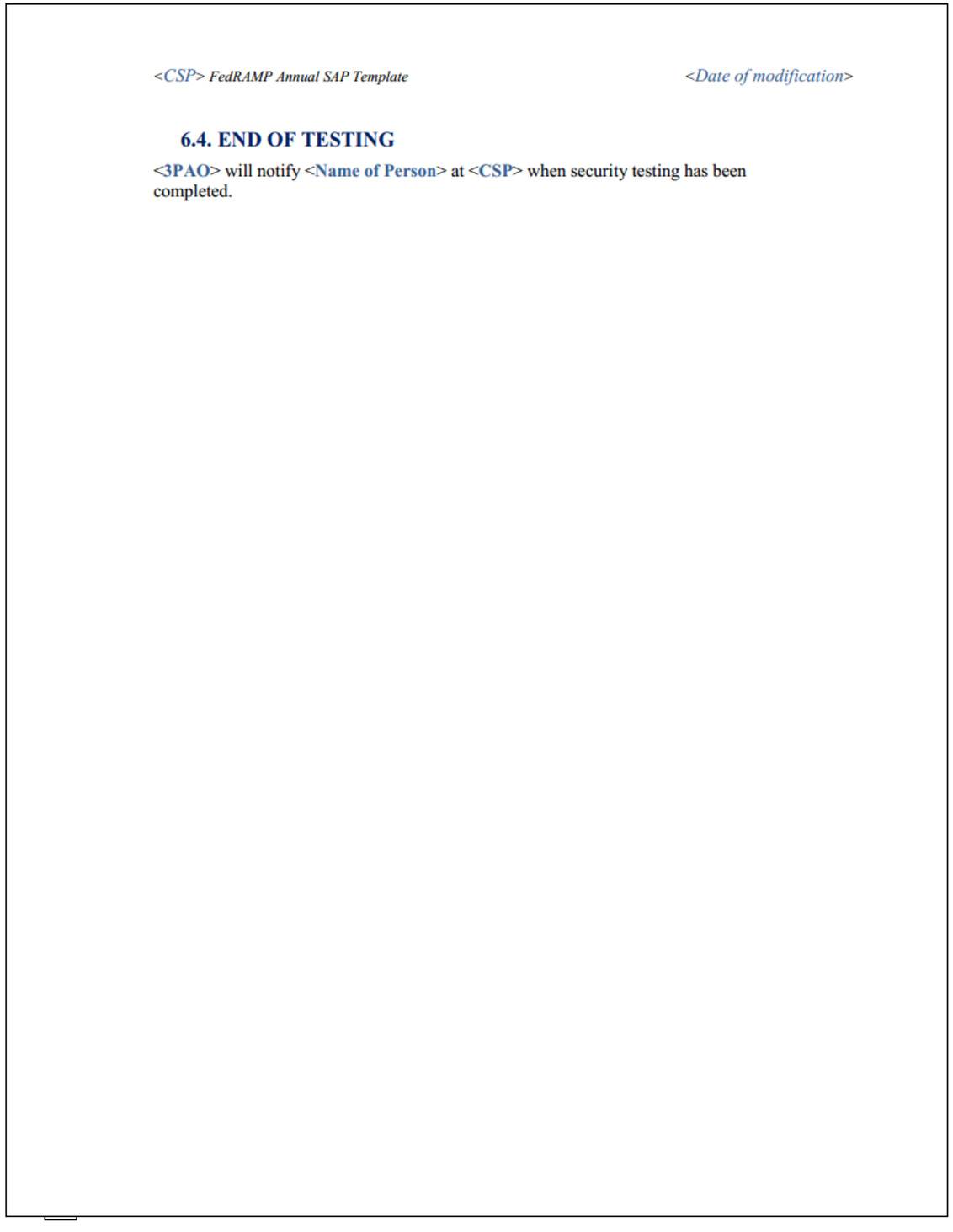
```
<terms-and-conditions>
   <part name="excluded-activities">
      <title>Excluded Activities</title>
      <p>The following activities are explicitly excluded from the assessment.</p>
      <part name="excluded-activity">
         <p>Changes to assigned user passwords</p>
      </part>
      <part name="excluded-activity">
         <p>Modification of user files or system files</p>
      </part>
      <part name="excluded-activity">
         <p>Telephone modem probes and scans (active and passive)</p>
      </part>
      <part name="excluded-activity">
         <p>Intentional viewing of [CSP Name] staff email, Internet caches, and/or personnel
            cookie files</p>
      </part>
      <part name="excluded-activity">
         <p>Denial of service attacks</p>
      </part>
      <part name="excluded-activity">
         <p>Exploits that will introduce new weaknesses to the system</p>
      </part>
      <part name="excluded-activity">
         <p>Intentional introduction of malicious code (viruses, Trojans, worms, etc.)</p>
      </part>
   </part>
<terms-and-conditions>
```

XPath Queries

```
(SAP) Number of Excluded Activities:
  count(/*/terms-and-conditions/part[@name='excluded-activities']/part[@name='excluded-
  activity'])

(SAP) First Excluded Activity:
  /*/terms-and-conditions/part[@name='excluded-activities']/part[@name='excluded-
  activity'][1]/node()

NOTE: Replace [1] as needed with [2], [3], etc.
```

NOTES:

- An assessment tool should present a list of included activities with a preceding phrase such as, "Security testing will not include any of the following activities:"



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

6.4. END OF TESTING

<3PAO> will notify <Name of Person> at <CSP> when security testing has been completed.

4.20. SAP ROE: End of Testing

This indicates who the Third Party Assessment Organization (3PAO) should notify within the CSP's organization when testing is complete.

Representation

```
   <metadata>
      <role id="csp-end-of-testing-poc">
         <title>CSP's End of Testing Notification POC</title>
         <desc>A role for an individual within the CSP to be notified by the assessor
when testing is complete.</desc>
      </role>

      <!-- Only define CSP party in SAP when no appropriate party exits in SSP -->

      <responsible-party role-id="csp-end-of-testing-poc">
         <!-- At Least one -->
         <party-uuid>person-2</party-uuid>
      </responsible-party>
   </metadata>
```

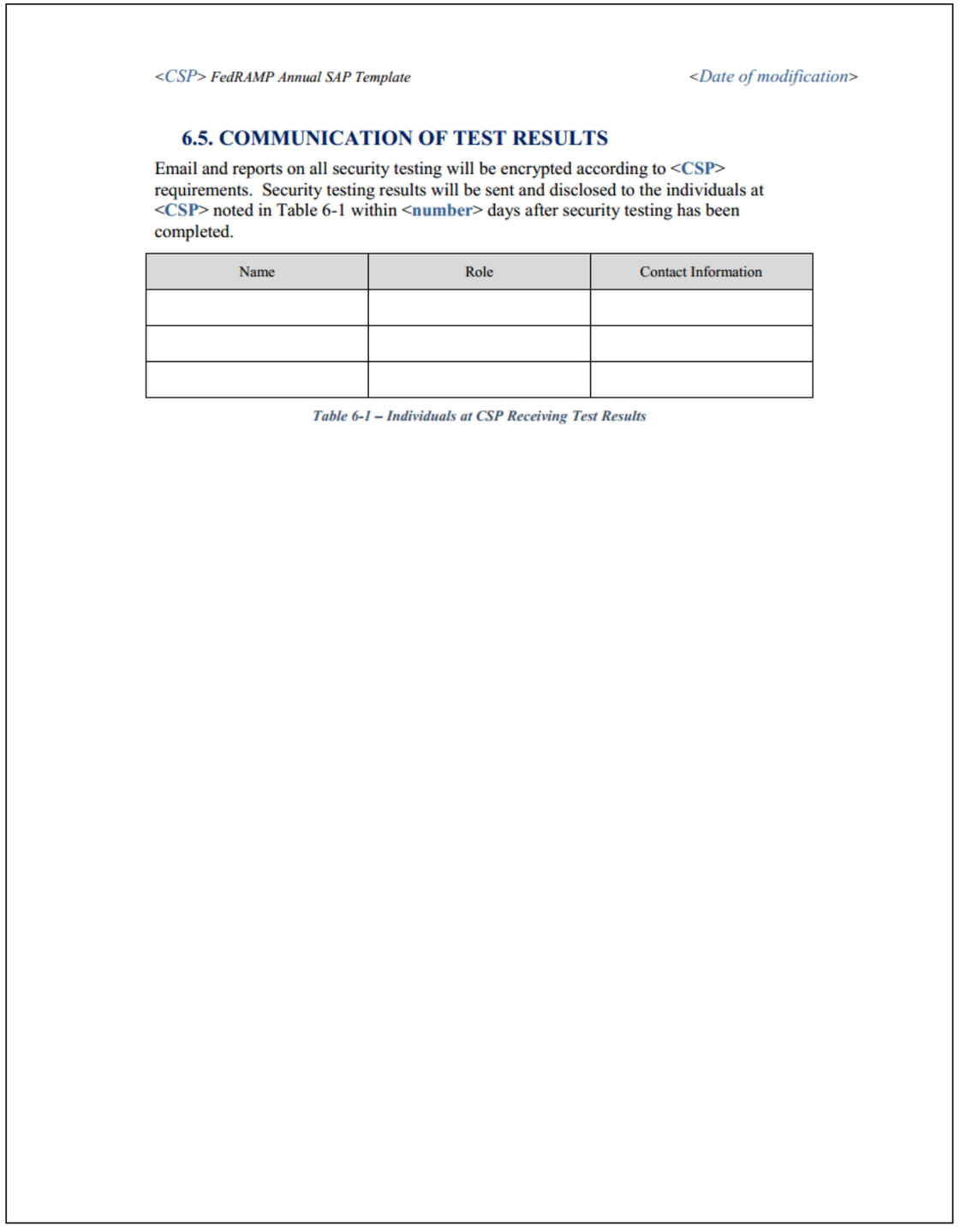
FedRAMP Defined Identifier
role ID: `csp-end-of-testing-poc`

XPath Queries

```
(SAP) Number of CSP Parties to notify at EOT (integer):
  count(/*/metadata/responsible-party[@role-id='csp-end-of-testing-poc']/party-uuid)

(SAP) ID of the first CSP Party to Notify:
  /*/metadata/responsible-party[@role-id='csp-end-of-testing-poc']/party-uuid[1]

NOTE: Replace [1] as needed with [2], [3], etc.

(SSP) Name of the first person or team:
  /*/metadata/party[@id='person-2']/(./person/person-name | ./org/org-name)

(SSP) Phone for the first person or team:
  /*/metadata/party[@id='person-2']//phone

(SSP) Email for the first person or team:
  /*/metadata/party[@id='person-2']//email

NOTE: Replace 'person-2' with each party-uuid found in the responsible role.
```

NOTES:

- IDs used for roles or parties in the SAP must not duplicate IDs used for roles or parties in the SSP.
- Only define a CSP party in the SAP when no appropriate party exists in the SSP.



<*CSP*> *FedRAMP Annual SAP Template* <*Date of modification*>

6.5. COMMUNICATION OF TEST RESULTS

Email and reports on all security testing will be encrypted according to <CSP> requirements. Security testing results will be sent and disclosed to the individuals at <CSP> noted in Table 6-1 within <number> days after security testing has been completed.

Name	Role	Contact Information

Table 6-1 – Individuals at CSP Receiving Test Results

4.21. SAP ROE: Communication of Test Results

Representation

```
   <metadata>
      <role id="csp-results-poc">
         <title>CSP Results POCs</title>
         <desc>A role for the individuals within the CSP who are to receive the
assessment results.</desc>
      </role>

      <!-- Only define CSP party in the SAP when no appropriate party exits in SSP -->

      <responsible-party role-id="csp-results-poc">
         <!-- One or More -->
         <party-uuid>person-1</party-uuid>
         <party-uuid>person-2</party-uuid>
      </responsible-party>
   </metadata>
```

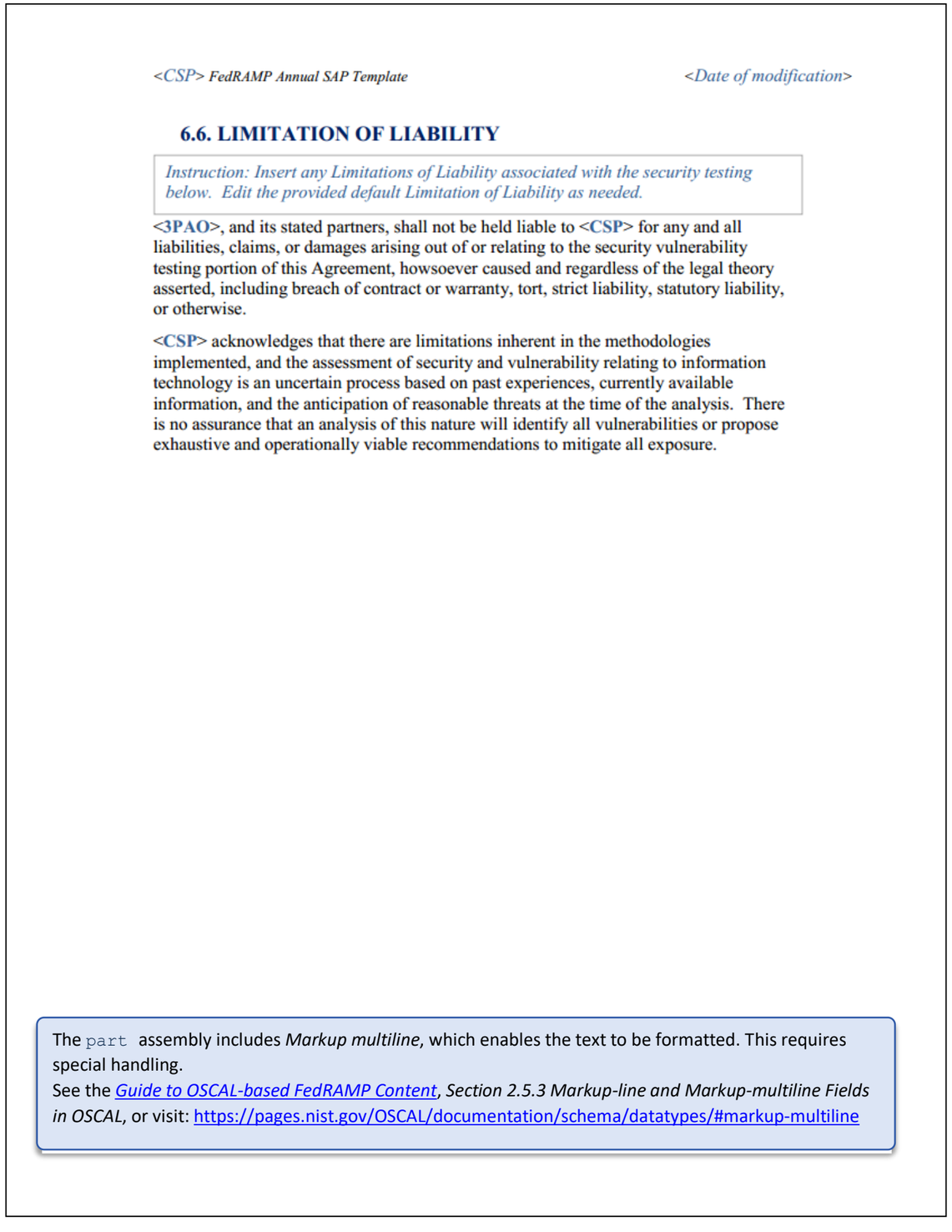
FedRAMP Defined Identifier
role ID: `csp-results-poc`

XPath Queries

```
(SAP) Number of CSP Test Result POCs (integer):
  count(/*/metadata/responsible-party[@role-id='csp-results-poc']/party-uuid)

(SAP) ID of the first CSP Assessment POC:
  /*/metadata/responsible-party[@role-id='csp-results-poc']/party-uuid[1]

NOTE: Replace [1] as needed with [2], [3], etc.

(SSP) Name of the first person or organization:
  /*/metadata/party[@id='person-1']/person/person-name

(SSP) Role/Title of the first person:
  /*/metadata/party[@id='person-1']/person/prop[@name='title']
  [@ns='https://fedramp.gov/ns/oscal']

(SSP) Phone for the first person or organization:
  /*/metadata/party[@id='person-1']//phone

(SSP) Email for the first person or organization:
  /*/metadata/party[@id='person-1']//email

NOTE: Replace 'person-1' with each party-uuid found in the responsible role.
```

NOTES:

- IDs used for roles or parties in the SAP must not duplicate IDs used for roles or parties in the SSP.
- Only define a CSP party in the SAP when no appropriate party exists in the SSP.



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

6.6. LIMITATION OF LIABILITY

Instruction: Insert any Limitations of Liability associated with the security testing below. Edit the provided default Limitation of Liability as needed.

<3PAO>, and its stated partners, shall not be held liable to **<CSP>** for any and all liabilities, claims, or damages arising out of or relating to the security vulnerability testing portion of this Agreement, howsoever caused and regardless of the legal theory asserted, including breach of contract or warranty, tort, strict liability, statutory liability, or otherwise.

<CSP> acknowledges that there are limitations inherent in the methodologies implemented, and the assessment of security and vulnerability relating to information technology is an uncertain process based on past experiences, currently available information, and the anticipation of reasonable threats at the time of the analysis. There is no assurance that an analysis of this nature will identify all vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate all exposure.

The `part` assembly includes *Markup multiline*, which enables the text to be formatted. This requires special handling.
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

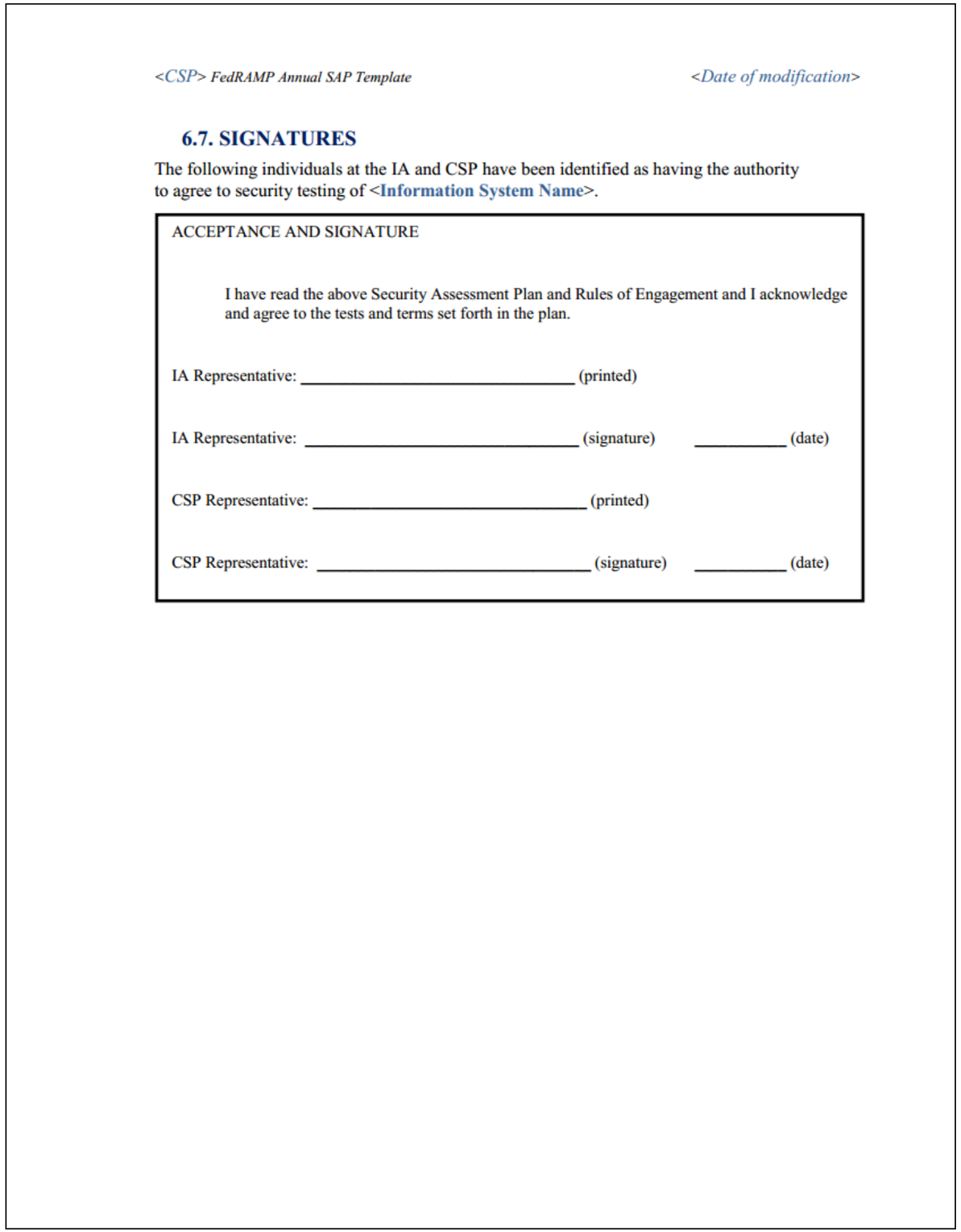
4.22. SAP ROE: Limitation of Liability

Representation

```
<terms-and-conditions>
   <part name="liability-limitations">
      <title>FedRAMP Required Limitation of Liability Statements</title>
      <part name="liability-limitation">
         <prop name="sort-id" value="001"/>
         <p>[3PAO Name], and its stated partners, shall not be held liable to [CSP Name]
            for any and all liabilities, claims, or damages arising out of or relating to
            the security vulnerability testing portion of this agreement, howsoever caused
            and regardless of the legal theory asserted, including breach of contract or
            warranty, tort, strict liability, statutory liability, or otherwise.</p>
      </part>
      <part name="liability-limitation">
         <prop name="sort-id" value="002"/>
         <p>[CSP Name] acknowledges that there are limitations inherent in the methodologies
            implemented, and the assessment of security and vulnerability relating to
            information technology is an uncertain process based on past experiences,
            currently available information, and the anticipation of reasonable threats
            at the time of the analysis. There is no assurance that an analysis of this
            nature will identify all vulnerabilities or propose exhaustive and
            operationally viable recommendations to mitigate all exposure.</p>
      </part>
</terms-and-conditions>
```

XPath Queries

```
(SAP) Count individual limitations of liability statements (integer):
  count(/*/terms-and-conditions/part[@name='liability-limitations']/
  part[@name='liability-limitation'])

(SAP) Obtain Sort IDs, for sorting by the SAP tool:
  /*/terms-and-conditions/part[@name='liability-limitations']/part[@name='liability-
  limitation'] /prop[@name='sort-id']

(SAP) The first liability limitation statement:
  /*/terms-and-conditions/part[@name='liability-limitations']/part[@name='liability-
  limitation']/prop [@name='sort-id'] [string()='001']/../(* except prop)

NOTE: Replace '001' with '002', '003', etc. for each sort-id based on desired order.
```



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

6.7. SIGNATURES

The following individuals at the IA and CSP have been identified as having the authority to agree to security testing of <Information System Name>.

ACCEPTANCE AND SIGNATURE

I have read the above Security Assessment Plan and Rules of Engagement and I acknowledge and agree to the tests and terms set forth in the plan.

IA Representative: _____ (printed)

IA Representative: _____ (signature) _____ (date)

CSP Representative: _____ (printed)

CSP Representative: _____ (signature) _____ (date)

4.23. SAP ROE: Signatures

Using a machine-readable format such as OSCAL for SAP content creates a challenge for handling of acceptance signatures. Early adopters are encouraged to approach the FedRAMP PMO to discuss specific solutions on a case-by-case basis. Until such time as the FedRAMP PMO and JAB have a well-established capability for handling signatures, one of the following approaches is encouraged:

- Manual "Wet" Signature Approach (Document or Letter)
- Digital Signature

Representation

```
<back-matter>
   <resource id="sap-signatures">
      <description><p>Signed SAP</p></description>
      <prop name='type' value='signed-sap'/>
      <!-- Use rlink and/or base64 -->
      <rlink href="./signed-sap.pdf" media-type="application/pdf" />
      <base64 filename="sap.pdf" media-type="application/pdf">00000000</base64>
   </resource>
</back-matter>
```

XPath Queries

```
(SAP) Link to signed SAP in PDF Format:
  /*/back-matter/resource/prop[@name='type'] [.='signed-sap']/../rlink/@href

(SAP) Base64-encoded signed SAP in PDF Format:
  /*/back-matter/resource/prop[@name='type'] [.='signed-sap']/../base64
```

4.23.1. Manual "Wet" Signature Approach (Document or Letter

Print, manually sign, scan, and attach.

1. Print one of the following:
    a. The OSCAL-based SAP content with a tool that renders the SAP in a format that resembles the MS-Word based FedRAMP SAP Template; or
    b. A separate letter, which uses the same language.
2. Have all parties manually sign the document or letter in ink.
3. Scan the signed copy.
4. Attach it to the OSCAL-based SAP as a resource.

4.23.2. Digital Signature Approach

Render, digitally sign, and attach.

1. Render the OSCAL-based SAP content as a PDF that resembles the MS-Word based FedRAMP SAP Template.
2. Have all parties digitally sign the PDF document.
3. Attach it to the OSCAL-based SAP as a resource.

<CSP> FedRAMP Annual SAP Template *<Date of modification>*

Appendix B – Security Test Case Procedures Template

Results shall be recorded in the FedRAMP Security Test Case Procedures Template.

Control Name	Control ID	Assessment Procedure	Assessment Objective	Examine	Interview	Test
Account Management | Disable Inactive Accounts	AC-2 (3)	AC-2(3).1	Determine if the organization: - defines the time period after which the information system automatically disables inactive accounts	Access control policy; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of temporary accounts removed and/or disabled; information system-generated list of emergency accounts removed and/or disabled; information system audit records; other relevant documents or		
	AC-2 (3)	AC-2(3).2	Determine if the information system: - automatically disables inactive accounts after the organization-defined time period		Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system	Automated mechanisms implementing account management functions
Account Management | Automated Audit Actions	AC-2 (4)	AC-2(4).1	Determine if the information system: - automatically audits the following account actions: - creation - modification - enabling - disabling - removal		Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities	Automated mechanisms implementing account management functions
	AC-2 (4)	AC-2(4).2	Determine if the organization: - defines personnel or roles to be notified of the following account actions: - creation - modification - enabling - disabling - removal	Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; notifications/alerts of account creation, modification, enabling, disabling, and removal actions; information system audit records; other relevant documents or		
	AC-2 (4)	AC-2(4).3	Determine if the information system: - notifies organization-defined personnel or roles of the following account actions: - creation - modification - enabling - disabling - removal		Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities	Automated mechanisms implementing account management functions
Account Management | Inactivity Logout	AC-2 (5)	AC-2(5).1	Determine if the organization: - defines either the time period of expected inactivity that requires users to log out or the description of when users are required to log out	Access control policy; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; security violation reports; information system audit records; other relevant documents or		

4.24. SAP Test Case Procedures

The assessment objectives and actions (Examine, Interview, and Test) from the test case workbook are now part of the OSCAL-based FedRAMP baselines, with the detail imported from the OSCAL-based NIST SP 800-53 Catalog via the baseline.

SAP and SAR Tools should be able to render Test Case Workbook objectives and actions using the OSCAL-based FedRAMP Baselines and NIST Catalog.

4.24.1. Baseline Objectives and Methods

To include an assessment objective and associated actions in the SAP, its control must be designated in-scope as described in *Sections 4.1, SAP Scope*. SAP tools should support and enforce this constraint.

In most cases, a FedRAMP assessor must adopt these without change. In this case, a SAP tool may simply specify all, to indicate that all assessment objectives should be included for all in-scope controls. If needed, objectives can be explicitly included or excluded as well.

Representation

```
<reviewed-controls>
   <control-selection>
      <description><h1>Control Scope</h1></description>
      <include-all />
      <exclude-control control-id="ac-1" />
   </control-selection>
   <control-objective-selection>
      <description><h1>Control Objective Scope</h1></description>
      <include-all />
      <!-- OR -->
      <include-objective objective-id="ac-1.a.1_obj.1" />
      <include-objective objective-id="ac-1.a.1_obj.2" />
      <include-objective objective-id="ac-1.a.1_obj.3" />
      <include-objective objective-id="ac-1.a.2_obj.1" />
      <include-objective objective-id="ac-1.a.2_obj.2" />
      <include-objective objective-id="ac-1.a.2_obj.3" />
      <include-objective objective-id="ac-1.b.1_obj.1" />
      <include-objective objective-id="ac-1.b.1_obj.2" />
      <include-objective objective-id="ac-1.b.2_obj.1" />
      <include-objective objective-id="ac-1.b.2_obj.2" />
   </control-objective-selection>
</reviewed-controls>
```

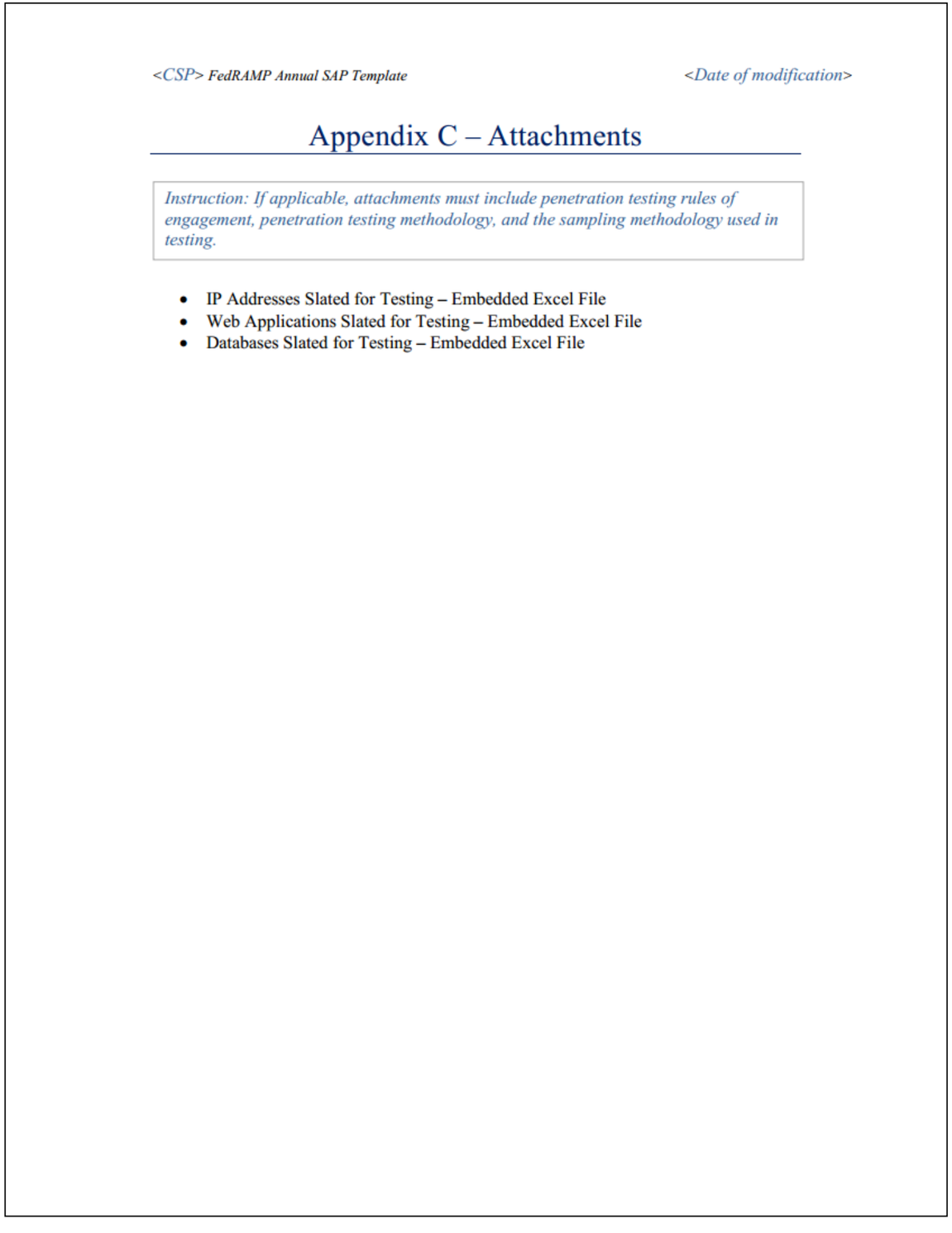
XPath Queries

```
(SAP) Include All Objectives for in-scope controls? (true or false):
  boolean(/*/reviewed-controls/control-objective-selection/include-all)

(SAP) Exclude Controls Specified? (true or false):
  boolean(/*/objectives/control-objectives/exclude-objective)

(SAP) Exclude Objectives Total (integer):
  count(/*/objectives/control-objectives/exclude-objective)

(SAP) Exclude Specific Objective (string):
  /*/objectives/control-objectives/exclude-objective[1]/@objective-id
```

Replace "[1]" with "[2]", "[3]", etc.

```
NOTE: Replace "exclude-objective" with "include-objective" above for any explicitly
  included objective; however, this is redundant when used with 'all'.
```

.



<CSP> FedRAMP Annual SAP Template *<Date of modification>*

Appendix C – Attachments

Instruction: If applicable, attachments must include penetration testing rules of engagement, penetration testing methodology, and the sampling methodology used in testing.

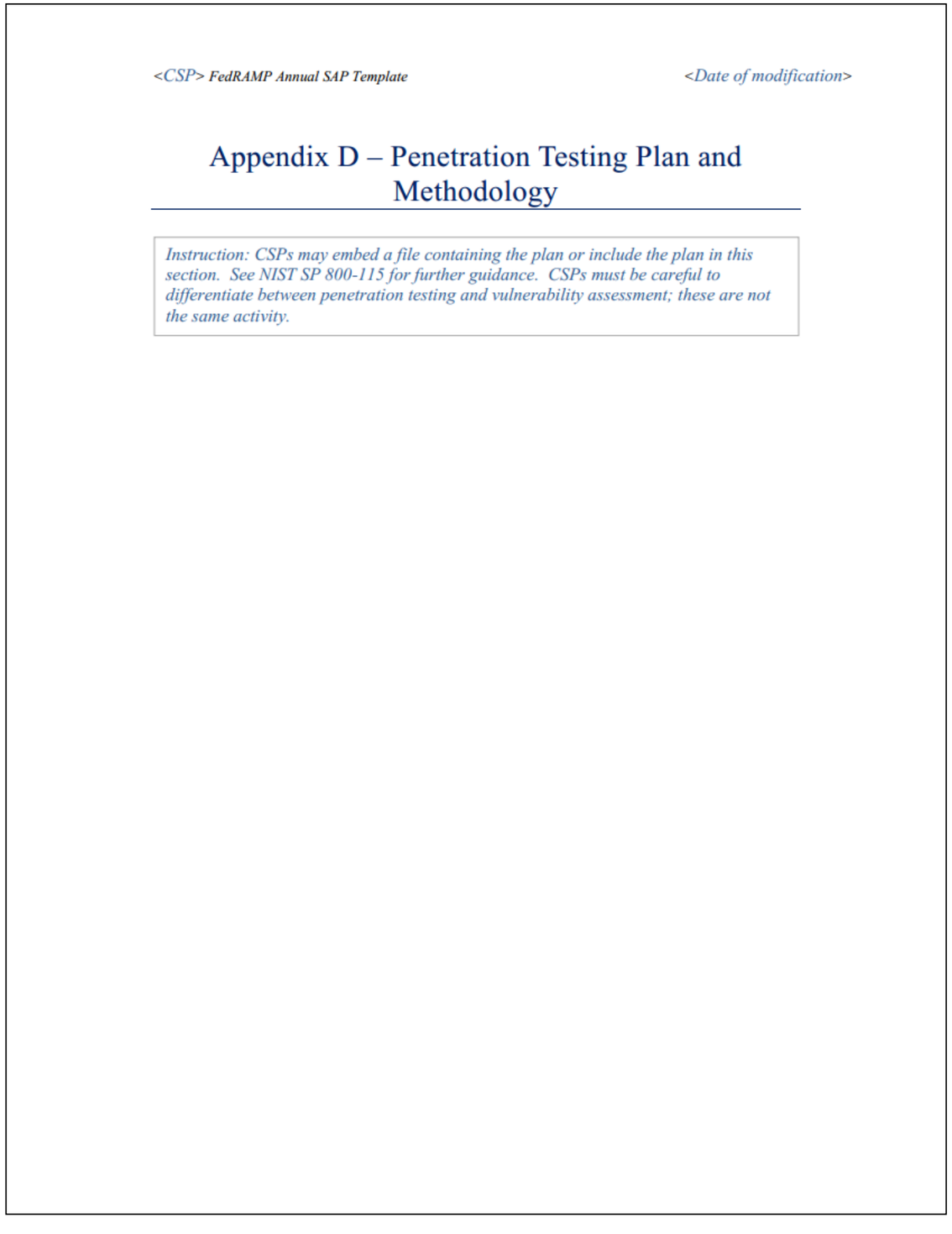
- IP Addresses Slated for Testing – Embedded Excel File
- Web Applications Slated for Testing – Embedded Excel File
- Databases Slated for Testing – Embedded Excel File

4.25. SAP Attachments

The content normally found in these three attachments can be modeled using OSCAL syntax, as described in:

- Section 4.4,SAP IP Addresses Slated for Testing;
- Section 4.5, SAP Web Applications Slated for Testing; and
- Section 4.6, SAP Databases Slated for Testing.

Please see those sections for more information.



<CSP> FedRAMP Annual SAP Template <Date of modification>

Appendix D – Penetration Testing Plan and Methodology

Instruction: CSPs may embed a file containing the plan or include the plan in this section. See NIST SP 800-115 for further guidance. CSPs must be careful to differentiate between penetration testing and vulnerability assessment; these are not the same activity.

4.26. SAP Penetration Testing Plan and Methodology

The penetration test plan methodology may continue to be a separate, attached document. The attachment must have the FedRAMP allowed value, `penetration-test-plan`.

Representation

```
<back-matter>
   <resource id="pen-test-plan">
      <desc>Penetration Test Plan</desc>
      <prop name='type'>penetration-test-plan</prop>
      <!-- Use rlink and/or base64 -->
      <rlink href="./pen_test_plan.pdf" media-type="application/pdf" />
      <base64 filename="pen_test_plan.pdf"
                              media-type="application/pdf">00000000</base64>
   </resource>
<back-matter>
```

FedRAMP Allowed Value

- `penetration-test-plan`

XPath Queries

```
(SAP) Link to Penetration Test Plan:
  /*/back-matter/resource/prop[@name='type'] [.='penetration-test-plan']/../rlink/@href

(SAP) Base64-encoded Penetration Test Plan:
  /*/back-matter/resource/prop[@name='type'] [.='penetration-test-plan']/../base64
```

5. GENERATED CONTENT

The following artifacts are historically generated by hand to summarize content found in other FedRAMP-required content. When using OSCAL, these artifacts can be generated from content found elsewhere. This includes the:

- **IP Addresses Slated for Testing**
- **Databases Slated for Testing**
- **Test Case Workbook**

If delivering FedRAMP content in OSCAL, assessors are no longer required to manually generate and maintain these artifacts, provided the content in their OSCAL-based FedRAMP SAP, and the CSP's OSCAL-based FedRAMP SSP remains accurate.

There are many ways a tool developer can generate these artifacts. FedRAMP is developing Extensible Stylesheet Language Transformation (XSLT) files to generate them. When ready, FedRAMP will make this freely available to the public here:

https://github.com/GSA/fedramp-automation/tree/master/resources

Tool developers are also encouraged to develop their own solutions to generating this content.

5.1. Generating the "IP Addresses Slated for Testing" List

The SAP must still identify the in-scope inventory items - either by reference or using the "all" clause. Once identified, the list of IP addresses slated for testing should be derived from the machine-readable inventory found in the SSP.

As described in *Section 4.4.1, If No OSCAL-based SSP Exists or Has Inaccurate Information (IP* Addresses), if the assessor finds SSP information inventory to be missing or inaccurate, the SAP tool must allow the assessor to insert inventory information into the `local-definitions` section of the SAP.

5.2. Generating the "Databases Slated for Testing" List

The SAP must still identify the in-scope inventory items - either by reference or using the "all" clause. Once identified, the list of Databases slated for testing should be derived from the machine-readable inventory found in the SSP.

As described in *Section 4.4.1, If No OSCAL-based SSP Exists or Has Inaccurate Information (IP* Addresses), if the assessor finds SSP information inventory to be missing or inaccurate, the SAP tool must allow the assessor to insert inventory information into the `local-definitions` section of the SAP.