|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | Guide to OSCAL-Based FedRAMP® Security Assessment Plans (SAP) – Rev5  User Implementation Guide  Fedramp2.0.0-oscal1.0.x  June 30, 2023 | |  |
|
|  |  | |  |
|  |  | Controlled Unclassified Information info@fedramp.gov  fedramp.gov |  |

TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 06/30/2023 | Fedramp2.0.0-oscal1.0.x | All | Initial release for FedRAMP rev 5 baselines SAP template. | FedRAMP PMO |
|  |  |  |  |  |

**How to contact us**

For questions about FedRAMP, or for questions about this document including how to use it, contact [info@FedRAMP.gov.](mailto:info@FedRAMP.gov)

For more information about FedRAMP, see [www.FedRAMP.gov](http://www.fedramp.gov).

TABLE OF CONTENTS

[1 Overview 1](#_Toc138945730)

[1.1 Who Should Use This Document? 1](#_Toc138945731)

[1.2 Related Documents 1](#_Toc138945732)

[1.3 Basic Terminology 1](#_Toc138945733)

[2 FedRAMP Extensions and Allowed Values 3](#_Toc138945734)

[3 Working with OSCAL Files 4](#_Toc138945735)

[3.1 XML and JSON Formats 4](#_Toc138945736)

[3.2 SAP File Concepts 4](#_Toc138945737)

[3.2.1 Resolved Profile Catalogs 6](#_Toc138945738)

[3.3 OSCAL-based FedRAMP SAP Template 7](#_Toc138945739)

[3.4 OSCAL’s SAP Minimum File Requirements 7](#_Toc138945740)

[3.5 Importing the System Security Plan 8](#_Toc138945741)

[3.5.1 When OSCAL-based SSP Information is Inaccurate 9](#_Toc138945742)

[3.5.2 If No OSCAL-based SSP Exists (General) 10](#_Toc138945743)

[3.6 Resolution Resource Prop 11](#_Toc138945744)

[4 SAP Template to OSCAL Mapping 12](#_Toc138945745)

[4.1 Background 14](#_Toc138945746)

[4.2 Scope 15](#_Toc138945747)

[4.2.1 Location of Components 16](#_Toc138945748)

[4.2.2 IP Addresses Slated for Testing 18](#_Toc138945749)

[4.2.3 SAP Web Applications Slated for Testing 21](#_Toc138945750)

[4.2.4 SAP Databases Slated for Testing 22](#_Toc138945751)

[4.2.4.1 If No OSCAL-based SSP Exists or Has Inaccurate Information (Database) 23](#_Toc138945752)

[4.2.5 Roles Testing Inclusions and Exclusion 24](#_Toc138945753)

[4.3 SAP Assumptions 26](#_Toc138945754)

[4.4 SAP Methodology 28](#_Toc138945755)

[4.5 Control Testing 30](#_Toc138945756)

[4.6 SAP Test Plan 31](#_Toc138945757)

[4.6.1 Assessor's Name, Address, and URL 31](#_Toc138945758)

[4.6.2 Security Assessment Team 33](#_Toc138945759)

[4.6.3 CSP Testing Points of Contact 34](#_Toc138945760)

[4.6.4 Testing Performed Using Automated Tools 35](#_Toc138945761)

[4.6.5 Testing Performed Through Manual Methods 36](#_Toc138945762)

[4.6.6 Schedule 38](#_Toc138945763)

[4.7 SAP Rules of Engagement (ROE) 39](#_Toc138945764)

[4.7.1 Origination Addresses 39](#_Toc138945765)

[4.7.2 Disclosures 40](#_Toc138945766)

[4.7.3 Security Testing May Include 41](#_Toc138945767)

[4.7.4 Security Testing Will Not Include 42](#_Toc138945768)

[4.7.5 End of Testing 43](#_Toc138945769)

[4.7.6 Communication of Test Results 44](#_Toc138945770)

[4.7.7 Limitation of Liability 45](#_Toc138945771)

[4.8 SAP Signatures 46](#_Toc138945772)

[4.8.1 Manual "Wet" Signature Approach (Document or Letter) Print, manually sign, scan, and attach. 46](#_Toc138945773)

[4.8.2 Digital Signature Approach Render, digitally sign, and attach. 47](#_Toc138945774)

[4.9 SAP Appendices 48](#_Toc138945775)

[4.9.1 Security Controls Selection Worksheet 48](#_Toc138945776)

[4.9.2 Test Case Procedures 48](#_Toc138945777)

[4.9.3 SAP Penetration Testing Plan and Methodology 50](#_Toc138945778)

[4.9.4 Significant Change Documentation 52](#_Toc138945779)

[5 Generated Content 53](#_Toc138945780)

[5.1 Generating the "IP Addresses Slated for Testing" List 53](#_Toc138945781)

[5.2 Generating the "Databases Slated for Testing" List 53](#_Toc138945782)

# Overview

## 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.

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

## 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.

The [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), 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)*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_System_Security_Plans_(SSP)_rev5.pdf).

## 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. |

# FedRAMP Extensions and Allowed Values

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

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.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf) 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*](https://github.com/GSA/fedramp-automation/raw/master/dist/content/rev5/resources/xml/FedRAMP_extensions.xml)
* [*JSON Version*](https://raw.githubusercontent.com/GSA/fedramp-automation/master/dist/content/rev5/resources/json/FedRAMP_extensions.json)
* [*HTML Version*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/FedRAMP_extensions.html)

# 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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf) provides important concepts necessary for working with any OSCAL-based FedRAMP file. Familiarization with those concepts is important to understanding this guide.

## 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.

## 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 to the left

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.

### Resolved Profile Catalogs

The resolved profile catalog for each FedRAMP baseline is produced by applying the FedRAMP profiles as a set of tailoring instructions on top of the NIST control catalog. 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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf) *Appendix C, Profile Resolution*.

## 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/dist/content/rev5/templates/sap/json/FedRAMP-SAP-OSCAL-Template.json>
* OSCAL-based FedRAMP SAP Template (XML Format):  
  [https://github.com/GSA/fedramp-automation/raw/master/dist/content/rev5/templates/sap/xml/FedRAMP-SAP-OSCAL-Template.xml](https://github.com/GSA/fedramp-automation/raw/master/dist/content/templates/sap/xml/FedRAMP-SAP-OSCAL-Template.xml)

## 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/](https://pages.nist.gov/OSCAL/concepts/layer/assessment/assessment-plan/)

## 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 universally unique identifier (UUID) value of a resource in the SAP file's back-matter. Refer to the [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, 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" value="system-security-plan"/>  <!-- Specify the XML or JSON file location. Only one required. -->  <rlink media-type="text/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.

### 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.

### 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 uuid="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="application/msword"/>  </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.

The **FedRAMP Logo** is base 64 encoded in the back-matter section of the OSCAL-based FedRAMP SSP Template, and can be referenced with the following XPath:

//back-matter/resource[@id='logo-fedramp']/base64

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.

## Resolution Resource Prop

FedRAMP will be implementing a separate set of automated SAP validation rules for the rev 5 OSCAL templates. To ensure FedRAMP initiates the appropriate validation rules when processing OSCAL SAPs, SAP authors should add a new prop called “resolution-resource” in the metadata section and include an associated back-matter resource as shown below:

|  |
| --- |
| SSP Resolution Resource |
| <assessment-plan>  <metadata>  <title>FedRAMP Security Assessment Plan (SAP)</title>  <!-- cut -->  <version>fedramp2.0.0-oscal1.0.4</version>  <oscal-version>1.0.4</oscal-version>  <revisions>  <revision>  <!-- cut -->  </revisions>  <!-- New rev 5 prop -->  <prop ns="https://fedramp.gov/ns/oscal" name="resolution-resource"  value="ace2963d-ecb4-4be5-bdd0-1f6fd7610f41" />  </metadata>  <!-- cut -->  <back-matter> <resource uuid="ace2963d-ecb4-4be5-bdd0-1f6fd7610f41">  <title>Resolution Resource</title>  <prop name="dataset" class="collection" value="Special Publication"/>  <prop name="dataset" class="name" value="800-53"/>  <prop name="dataset" class="version" value="5.0.2"/>  <prop name="dataset" class="organization" value="gov.nist.csrc"/>  <remarks>  <p>This "resolution resource" is used by FedRAMP as a local, authoritative indicator of what version SAP (rev 4 or rev 5) this OSCAL document is for.</p>  </remarks>  </resource>  </back-matter>  </ assessment-results> |
| XPath Queries |
| (SAR) UUID of “resolution-resource”: /\*/metadata/prop[@name=”resolution-resource”]/@value  (SAR)Target baseline version: /\*/back-matter/resource[@uuid=”uuid-of-resolution-resource”]/prop[@name=”dataset” and @class=”version”]/@value |

If the “resolution-resource” prop is not specified in the metadata section of the SAP, FedRAMP will assume the SAP should be validated using the rev 5 validation rules. If the “resolution-resource” prop is present, FedRAMP will use the validation rules that correspond with the version specified in the back-matter resource.

# 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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*.* This includes the following:

|  |  |
| --- | --- |
| **Topic** | **Location** |
| Title Page | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 4.1* |
| Prepared By/For | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 4.2 - 4.4* |
| Record of Template reChanges | Not Applicable. Instead follow [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 2.3.2, OSCAL Syntax Version* |
| Revision History | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 4.5* |
| How to Contact Us | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 4.6* |
| Document Approvers | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 4.7* |
| Acronyms and Glossary | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 4.8* |
| Laws, Regulations, Standards and Guidance | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, Section 4.9* |
| Attachments and Citations | [*Guide to OSCAL-based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf)*, 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.

**NOTE: The FedRAMP SAP template screenshots in the sections that follow vary slightly from the most current version of the FedRAMP rev 5 SAP template.**

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

## Text, letter Description automatically generatedBackground

The *Background*, *Purpose*, and *Applicable Laws* sections of the FedRAMP SAP template contain references to the CSP name, the CSO name, and the independent assessor (IA) name. The information in these sections may be represented as a part assembly within the terms-and-conditions element of an OSCAL SSP. This approach is optional as the specific data items can simply be queried from an OSCAL SAP and its associated documents.

**Background Section Content**

Capturing the SAP *background*, *purpose*, and *applicable laws* prose in OSCAL is not required by FedRAMP but may be useful for scenarios where rendering the content in human-readable format is desired (e.g., converting the OSCAL SAP to a formatted PDF or Word document). If the content is not captured within the OSCAL terms-and-conditions assembly, conversion tools can query the OSCAL SAP (and associated SSP) for specific data items such as the IA name, the CSP name, the CSO name, etc.

|  |
| --- |
| Representation |
| <!-- cut -->   <terms-and-conditions>  <!-- Section 2 Background -->  <part ns="https://fedramp.gov/ns/oscal" name="background">  <title>Background</title>  <p>Insert text from FedRAMP template</p>  <p> Insert text from FedRAMP template </p>  <part ns="https://fedramp.gov/ns/oscal" name="nist-sp800-39">  <p> Insert text from FedRAMP template</p>  </part>  <!-- Section 2.1 -->  <part ns="https://fedramp.gov/ns/oscal" name="purpose">  <title>Purpose</title>  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="001"/>  <p>This SAP has been developed by [IA Name] and is for [an initial assessment/an annual assessment/an annual assessment and significant change assessment/a significant change assessment] of the [CSP Name], [CSO Name]. The SAP provides the goals for the assessment and details how the assessment will be conducted.</p>  </part>  <!-- Section 2.2 -->  <part ns="https://fedramp.gov/ns/oscal" name="laws-regulations" >  <title>Applicable Laws, Regulations, Standards and Guidance</title>  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="002"/>  <p>The FedRAMP-applicable laws, regulations, standards and guidance is included in the [CSO Name] SSP section – System Security Plan Approvals. Additionally, in Appendix L of the SSP, the [CSP Name] has included laws, regulations, standards, and guidance that apply specifically to this system.</p>  </part>  </part>  <!-- cut -->  </terms-and-conditions> |
| XPath Queries |
| (SAP) IA Name: /assessment-plan/metadata/party[@uuid="uuid-of-ia"]/name  (SAP) Initial assessment, annual assessment, or significant change? /assessment-plan/metadata/prop[@ns="https://fedramp.gov/ns/oscal" and @name="assessment-type"]/@value  (SAP) Are there no/one/many significant changes in SAP scope? /assessment-plan/metadata/prop[@ns="https://fedramp.gov/ns/oscal" and @name="significant-changes-scope"]/@value  (SAP) CSP Name: /assessment-plan/metadata/party[@uuid="uuid-of-csp"]/name  (SSP) CSO Name: /system-security-plan/system-characteristics/system-name |

## Graphical user interface, text, application, email Description automatically generatedScope

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 |

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.

**NOTE:**

See *Section 4.1, Background* for information on how to capture SAP scope information within the OSCAL terms-and-conditions assembly and how to query the OSCAL SAP (and associated SSP) for specific data items such as the IA name, the CSP name, the CSO name, etc.

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

### Table Description automatically generatedLocation of Components

The SAP reference 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.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

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

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.

See Previous 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.

### Graphical user interface, text, application Description automatically generatedIP 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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_System_Security_Plans_(SSP)_rev5.pdf) 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.

**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.

|  |
| --- |
| 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" type="token" /> </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"  type="token" />  <exclude-subject subject-uuid="uuid-of-SSP-inventory-item-to-exclude"  type="token" /> </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"  type="token" />  <include-subject subject-uuid="uuid-of-SSP-inventory-item-to-include"  type="token" />  <include-subject subject-uuid="uuid-of-SSP-inventory-item-to-exclude"  type="token" /> </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'] |

Graphical user interface, text, application

Description automatically generated

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

#### Graphical user interface, text, application Description automatically generatedIf 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"  type="token" />  <exclude-subject subject-uuid="uuid-of-SAP-inventory-item-to-include"  type="token" /> </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 |

### Graphical user interface, text, application Description automatically generatedSAP 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)*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_System_Security_Plans_(SSP)_rev5.pdf) 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.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| Representation |
| <local-definitions>  <activity uuid="uuid-of-web-application-activity">  <title>Web Application Test #1</title>  <description><p>Describe this web application test.</p></description>  <prop name="type" ns="https://fedramp.gov/ns/oscal" value="web-application"/>  </activity> </local-definitions> <!-- cut: terms-and-conditions, reviewed-controls, assessment-subject --> <task uuid="task-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"/>  <associated-activity activity-uuid="uuid-of-web-application-activity">  <subject type="inventory-item">  <include-subject subject-uuid="uuid-of-SSP-inventory-item"  type="inventory-item" />  </subject>  </associated-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]/ associated-activity/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. |

Graphical user interface, text, application

Description automatically generated

### 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)*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_System_Security_Plans_(SSP)_rev5.pdf) 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] |

### 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.

### Graphical user interface, text, application, email Description automatically generatedRoles Testing Inclusions and Exclusion

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 must ensure all roles are included for testing and identify roles excluded from testing. When processing an OSCAL SAP, SAP tools should present assessors with the roles from the associated (import-ssp) SSP so the assessor can select specific roles for testing. SAP tools should allow the assessor to easily identify roles that are excluded. Section 6.2 of the [*Guide to OSCAL-based System Security Plans (SSP)*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_System_Security_Plans_(SSP)_rev5.pdf) describes personnel roles and privileges with examples illustrating how to identify them in an OSCAL SSP. If the "roles" slated for testing exist in the SSP, the SSP roles are referenced from the SAP using their SSP IDs as defined in the SSP user assemblies in the system-implementation section of the OSCAL-based SSP file. **Note that in this case, the SAP role must actually map to the uuid of the user assembly in the SSP**.

Assessors should ensure the selection of at least one SSP-defined role from each of the common generalized role categories (“internal”, “external”, and “privileged”). If the assessor elects to reference more generic roles, the SAP tool should enable the assessor to create these generic roles locally in the SAP local-definitions assembly.

|  |
| --- |
| Representation |
| <local-definitions>  <!—add user assembly for each role to be assessed 🡪  <user uuid=”uuid-value”>  <title>Assessor Specified Role</title>  <prop name=”sensitivity” ns=”https://fedramp.gov/ns/oscal” value=”limited” />  <prop name=”type” value=”external”/>  <prop name=”privilege-level” value=”no-logical-access” />  <role-id>id-for-assessor-specified-role</role-id>  <authorized-privilege>  <title>Full administrative access (root)</title>  <function-performed>Add/remove users and hardware</function-performed>  <function-performed>install and configure software</function-performed>  <function-performed>OS updates, patches and hotfixes</function-performed>  <function-performed>perform backups</function-performed>  </authorized-privilege>  </user> </local-definitions> |

For every role to be tested, whether pre-identified in the SSP or identified by the assessor, there must be an assessment-subject entry, and at least one corresponding task. A SAP tool should enable the assessor to add a test user ID here via FedRAMP extension properties.

|  |
| --- |
| Representation |
| <assessment-plan>   <!-- cut metadata -->  <!-- cut import-ssp, local-definitions, terms-and-conditions, reviewed-controls -->  <!-- set type to 'user' -->  <assessment-subject type="user">  <description>  <p>A description of the included roles.</p>  <p>A description of an excluded role.</p>  </description>  <!-- uuid from SSP or SAP lcocal-definitions -->  <include-subject subject-uuid="user-uuid-from-SSP" type="token" />  <exclude-subject subject-uuid="user-uuid-from-SSP" type="token" />  </assessment-subject>   <!-- cut assessment-assets -->  <task uuid="task-uuid" type="action">  <title>Role-Based Tests</title>  <task uuid="test1-uuid" type="action">  <title>Role Based Test #1</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-user"/>  <!-- uuid from SSP or SAP lcocal-definitions -->  <prop name="user-uuid"  ns="https://fedramp.gov/ns/oscal"  value="user-uuid-value"/>  <associated-activity activity-uuid="uuid-of-role-testing-activity" />  </task>  <task uuid="test2-uuid" 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"/>  <!-- uuid from SSP or SAP lcocal-definitions -->  <prop name="user-uuid" ns="https://fedramp.gov/ns/oscal"  value="user-uuid-value"/>  <associated-activity activity-uuid="uuid-of-role-testing-activity" />  </task>  </task>  <!-- cut back-matter --> </assessment-plan> |

.

## Text, letter Description automatically generatedSAP 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.

The insert elements can be used by tool developers as insertion points for data items that the tool may manage as parameters. The use of insert within an OSCAL part is described on the [NIST OSCAL Concepts page](https://pages.nist.gov/OSCAL/concepts/layer/control/catalog/sp800-53rev5-example/#parts).

|  |
| --- |
| Representation |
| <terms-and-conditions>  <part name="assumptions">  <part name="assumption">  <prop name="sort-id" value="001"/>  <p>This SAP is based on <insert type="param" id-ref="cso\_name\_prm"/>...</p>  </part>  <part name="assumption">  <prop name="sort-id" value="002"/>  <p>The <insert type="param" id-ref="csp\_name\_prm"/> ... </p>  </part>  <part name="assumption">  <prop name="sort-id" value="003"/>  <p>The <insert type="param" id-ref="ia\_name\_prm"/> ... </p>  </part>  <part name="assumption">  <prop name="sort-id" value="004"/>  <p>The <insert type="param" id-ref="csp\_name\_prm"/>... </p>  </part>  <part name="assumption">  <prop name="sort-id" value="005"/>  <p>Security controls that ... on these security controls.</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:**

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

* 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.

## Graphical user interface, text, application Description automatically generatedGraphical user interface, text, application Description automatically generatedSAP Methodology

In general, the methodology is simply a single markup multiline field, which enables the assessor to modify the content using rich text formatting. The FedRAMP SAP template includes subsections for *Control Testing, Data Gathering, Sampling,* and *Penetration Test*. Each of these sections must be present in the FedRAMP OSCAL SAP terms-and-condition assembly, within part named ”methodology” as sub-parts. The subparts are specifically defined for FedRAMP SAP, so they have namespace “https://fedramp.gov/ns/oscal” and attributes are named “control-testing”, “data-gathering”, “sampling”, and “pen-testing”.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| Representation |
| <terms-and-conditions>  <!-- Section 5 -->  <part name="methodology">  <title>Methodology</title>  <!-- Section 5.1 Control Testing -->  <part ns="https://fedramp.gov/ns/oscal" name="control-testing">  <title>Control Testing</title>  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="001"/>  <p>[IA Name] will ... </p>  </part>  <!-- Section 5.2 Data Gathering -->  <part ns="https://fedramp.gov/ns/oscal" name="data-gathering">  <title>Data Gathering</title>  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="002"/>  <p>[IA Name] data gathering activities will ... </p>  </part>  <!-- Section 5.3 Sampling -->  <part ns="https://fedramp.gov/ns/oscal" name="sampling">   <title>Sampling</title>  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="003"/>  <prop ns="https://fedramp.gov/ns/oscal" name="sampling" value="no"/>  <p>The sampling methodology for evidence/artifact gathering, related to controls assessment, is described in Appendix B.</p>  <p>[IA Name] [will/will not] ... </p>  </part>  <!-- Section 5.4 Penetration Test -->  <part ns="https://fedramp.gov/ns/oscal" name="pen-testing">  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="004"/>  <p>The Penetration Test Plan and Methodology is attached in Appendix C.</p>  </part>  </part>  <!-- cut --> </terms-and-conditions> |

Graphical user interface, text, application, email

Description automatically generatedFedRAMP requires the presence of the sampling property, which indicates whether sampling will be used by the assessor for the assessment. The insert elements can be used by tool developers for insertion points for data items that the tool may manage as parameters. CSP tools must display a definitive statement based on the value of the sampling property.

**FedRAMP Extension (Sampling Plans)**

prop (ns="https://fedramp.gov/ns/oscal"):

* name="sampling"

|  |
| --- |
| Representation |
| <terms-and-conditions>  <!-- Section 5 -->  <part name="methodology">  <title>Methodology</title>   <!-- Section 5.3 Sampling -->  <part ns="https://fedramp.gov/ns/oscal" name="sampling">   <title>Sampling</title>  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="003"/>  <prop ns="https://fedramp.gov/ns/oscal" name="sampling" value="no"/>  <p>The sampling methodology for evidence/artifact gathering, related to controls assessment, is described in Appendix B.</p>  <p>[IA Name] [will/will not] ... </p>  </part>  </part>  <!-- cut --> </terms-and-conditions> |
| 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.

## Control Testing

**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.

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.

**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’/>)

|  |
| --- |
| 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 -->   </control-selection>  <!-- control-objectives -->  <!-- objectives -->  <control-objective-selection><!-- cut --></control-objective-selection> </reviewed-controls> <!-- 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)  Replace "[1]" with "[2]", "[3]", etc.  (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'. |

**NOTES:**

* Tools should validate the control IDs for explicitly included or excluded controls using the relevant baseline.

The **FedRAMP Logo** is base 64 encoded in the back-matter section of the OSCAL-based FedRAMP SSP Template, and can be referenced with the following XPath:

//back-matter/resource[@id='logo-fedramp']/base64

* FedRAMP's guidance and requirements regarding which controls are in-scope for each assessment does not change with OSCAL.

## Graphical user interface, text, application, email Description automatically generatedSAP Test Plan

### Assessor's Name, Address, and URL

Table

Description automatically generated with low confidenceThe 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-uuid>  <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 Extension (A2LA Certification #)**  prop (ns="https://fedramp.gov/ns/oscal"):   * name="iso-iec-17020-identifier"   **FedRAMP Defined Identifier**  role ID: assessor |
| 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'] |

### Graphical user interface, text, application, email Description automatically generatedSecurity 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. |

### Graphical user interface, application Description automatically generated with medium confidenceCSP 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.

### Table Description automatically generated with medium confidenceTesting 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.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| Representation |
| <assessment-assets >  <component uuid="assessor-component1-uuid" 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="assessor-componenet2-uuid" 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"/>  <remarks><p><!-- cut --></p></remarks>  </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 FedRAMP, assessment tools state should typically be 'operational', otherwise a remark must be provided.

### Table Description automatically generatedTesting Performed Through Manual Methods

In OSCAL, the manual assessment methods are described in the activity assembly as shown below:

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| 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" value="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, indicating each type.

#### Table Description automatically generated Including Manual Test Methods in the OSCAL SAP Test Plan Section

The FedRAMP OSCAL SAP terms-and-condition assembly, should contain a part with ns="https://fedramp.gov/ns/oscal" name="manual-methods-testing" when needed to facilitate rending of OSCAL SAP by tools. The insert elements can be used by tool developers as insertion points for data items such as test ID, test name, and test description if the tool is able manage them as parameters. The use of insert within an OSCAL part is described on the [NIST OSCAL Concepts page](https://pages.nist.gov/OSCAL/concepts/layer/control/catalog/sp800-53rev5-example/#parts). The XPath queries below show how to identify manual test information within the OSCAL SAP.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| Representation |
| <terms-and-conditions>  <!-- Section 6 Test Plan -->  <part ns="https://fedramp.gov/ns/oscal" name="test-plan">  <title>Test Plan</title>  <!-- Section 6.4 Testing performed using manual methods -->  <part ns="https://fedramp.gov/ns/oscal" name="manual-methods-testing">  <title>Testing Performed Using Manual Methods</title>  <prop ns="https://fedramp.gov/ns/oscal" name="sort-id" value="004"/>  <!-- Table 6-4 Describe what technical tests will be performed through manual methods without the use of automated tools. -->  <table>  <tr>  <th>Test ID</th>  <th>Test Name</th>  <th>Description</th>  </tr>  <tr>  <!-- Identifiers must be in the format MT-1, MT-2, etc., which indicates "Manual Test 1", "Manual Test 2", etc. -->  <td>[Insert test ID]</td>  <td>[Insert test name]</td>  <td>[Insert test description text]</td>  </tr>  </table>  </part>  </part>  <!-- cut --> </terms-and-conditions> |
| XPath Queries |
| (SAP) Test ID: /assessment-plan/local-definitions[1]/activity[1]/prop[@ns="https://fedramp.gov/ns/oscal" and @name="label"]/@value  (SAP) Test Name: /assessment-plan/local-definitions[1]/activity[1]/title  (SAP) Description: /assessment-plan/local-definitions[1]/activity[1]/description/p  NOTE: Replace [1] as needed with [2], [3], etc. |

### Table Description automatically generatedSchedule

In OSCAL, the assessment schedule is described using an array of task assemblies as shown below:

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

|  |
| --- |
| 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](https://pages.nist.gov/OSCAL/reference/datatypes/#date-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.

## 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.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| 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.

### Graphical user interface, text, application, email Description automatically generatedDisclosures

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

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| 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.

### Text, letter Description automatically generatedSecurity Testing May Include

SAP authors should describe the security testing that may be included within the terms-and-conditions assembly, in the “included-activities” part and its “included-activity” sub-parts.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| 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>  <!-- cut other included-activities -->  </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:"

### Graphical user interface, text, application, letter, email Description automatically generatedSecurity Testing Will Not Include

SAP authors should describe exclusive disclosures within the terms-and-conditions assembly, in the “excluded-activities” part and its “included-activity” sub-parts.

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| 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:"

### Text, letter Description automatically generatedEnd of Testing

This indicates who the Independent Assessor (IA) 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.

### Text, letter Description automatically generatedCommunication of Test Results

This indicates who the Independent Assessor (IA) should send all the assessment results to at the CSP's organization.

|  |
| --- |
| 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.

### Text, letter Description automatically generated Limitation of Liability

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*](https://github.com/GSA/fedramp-automation/raw/master/documents/rev5/Guide_to_OSCAL-based_FedRAMP_Content_rev5.pdf), *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline>

|  |
| --- |
| 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><insert type="param" id-ref="3pao\_name\_prm"/>, and its stated partners, shall not be held liable to <insert type="param" id-ref="csp\_name\_prm"/> 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><insert type="param" id-ref="csp\_name\_prm"/> 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>  </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. |

## Table Description automatically generatedSAP Signatures

Using a machine-readable format such as OSCAL for SAP content creates a challenge in the 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 |

### Manual "Wet" Signature Approach (Document or Letter) Print, manually sign, scan, and attach.

1. Print one of the following:
   1. 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
   2. 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.

### 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.

## SAP Appendices

### Security Controls Selection Worksheet

An OSCAL SAP must always explicitly select the in-scope controls from the applicable FedRAMP Baseline/Profile. See section 4.5 Controls Testing for additional guidance.

### 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](https://github.com/GSA/fedramp-automation/tree/master/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.

#### 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'. |

A picture containing table

Description automatically generated.

### 

#### Sampling Methodology

The sampling methodology may continue to be a separate, attached document. This should be provided as a back-matter resource, containing a FedRAMP “type” prop with an allowed value, sampling-methodology.

|  |
| --- |
| Representation |
| <back-matter>  <resource uuid="uuid">  <title>Sampling Methodology</title>  <description>  <p>Embed or reference copies of the sampling methodology for security controls assessment and vulnerability scanning (if applicable).</p>  </description>  <prop ns="https://fedramp.gov/ns/oscal" name="type"  **FedRAMP Allowed Value**   * sampling-methodology   value="sampling-methodology"/>  <!-- Use rlink and/or base64 -->  <rlink href="./sampling-methodology-reference-1.pdf"  media-type="application/pdf"/>  <rlink href="./sampling-methodology-reference-2.docx"  media-type="application/msword"/>  </resource> <back-matter> |
| XPath Queries |
| (SAP) Link to Sampling Methodology: /\*/back-matter/resource/prop[@name='type'] [@value='sampling-methodology']/../rlink/@href  (SAP) Base64-encoded Sampling Methodology: /\*/back-matter/resource/prop[@name='type'] [@value=''sampling-methodology ']/../base64 |

### SAP Penetration Testing Plan and Methodology

The penetration test plan methodology may continue to be a separate, attached document. This should be provided as a back-matter resource, containing a FedRAMP “type” prop with an allowed value, penetration-test-plan.

|  |
| --- |
| Representation |
| <back-matter>  <resource uuid="uuid">  <title>Penetration Testing Plan and Methodology</title>  <description>  <p> . . . /p>  <!-- update the table to reflect the attack vectors, threat models,  and attack models being assessed. -->  <table>  <tr>  <th>Include</th>  <th>Mandatory Attack Vectors</th>  <th>Include</th>  <th>Threat Models</th>  <th>Include</th>  <th>Attack Models</th>  </tr>  <tr>  <td>x</td>  <td>External to Corporate</td>  <td></td>  <td>Internet based (untrusted)</td>  <td></td>  <td>Enterprise</td>  </tr>  <tr> . . . </tr>  </table>  </description>  <prop ns="https://fedramp.gov/ns/oscal" name="type"  **FedRAMP Allowed Value**   * penetration-test-plan   value="penetration-test-plan"/>  <!-- 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> |
| XPath Queries |
| (SAP) Link to Penetration Test Plan: /\*/back-matter/resource/prop[@name='type'] [@value='penetration-test-plan']/../rlink/@href  (SAP) Base64-encoded Penetration Test Plan: /\*/back-matter/resource/prop[@name='type'] [@value='penetration-test-plan']/../base64 |

### Significant Change Documentation

The significant change documentation must be provided as a back-matter resource, containing a FedRAMP “type” prop with an allowed value, significant-change-request.

|  |
| --- |
| Representation |
| <back-matter> <!-- Significant Change Request Documentation -->  <resource uuid="c965ffb0-cd67-4a80-9014-0c7a217c1f85">  <title>Significant Change Request Documentation</title>  <description>  <p><tr> . . . </tr></p>  <!-- Add table of additional roles -->  <table>  <tr>  <th>Role Name</th>  <th>Test User ID</th>  <th>Associated Functions</th>  </tr>  <tr> . . . </tr>  </table>  </description>  <prop ns="https://fedramp.gov/ns/oscal" name="type"  **FedRAMP Allowed Value**   * significant-change-request   value="significant-change-request"/>  <!-- Use rlink and/or base64 -->  <rlink href="./fedramp\_scr\_form.pdf" media-type="application/pdf"/>  <rlink href="./scr\_inventory.xlsx" media-type="application/vnd.ms-excel"/>  <rlink href="./other\_scr\_files.zip" media-type="application/zip"/>  </resource>  <back-matter> |
| XPath Queries |
| (SAP) Link to Significant Change Documentation: /\*/back-matter/resource/prop[@name='type'] [@value=' significant-change-request ']/../rlink/@href  (SAP) Base64-encoded Significant Change Documentation: /\*/back-matter/resource/prop[@name='type'] [@value= significant-change-request ']/../base64 |

# 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/dist/content/resources>

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

## 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.

## 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.