Guide to OSCAL-Based FedRAMP® System Security Plans (SSP) – Rev5

User Implementation Guide

Fedramp2.0.0-oscal1.0.x

June 30, 2023

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 SSP 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.

For more information about FedRAMP, see www.FedRAMP.gov.

TABLE OF CONTENTS

1. Overview

1.1. Who Should Use This Document?

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

It provides guidance and examples intended to guide an organization in the production and use of OSCAL-based FedRAMP-compliant SSP 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 SSP content and accuracy rather than formatting and presentation.

1.2. Related Documents

This document does not stand alone. It provides information specific to developing tools to create and manage OSCAL-based, FedRAMP-compliant SSPs.

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

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

1.3. Basic Terminology

XML and JSON use different terminology. Instead of repeatedly clarifying format-specific terminology, this document uses the following format-agnostic terminology through the document.

TERM	XML EQUIVALENT	JSON EQUIVALENT
`Field`	A single element or node that can hold a value or an attribute	A single object that can hold a value or property
`Flag`	Attribute	Property
`Assembly`	A collection of elements or nodes. Typically, a parent node with one or more child nodes.	A collection of objects. Typically, a parent object with one or more child objects.

These terms are used by National Institute of Standards and Technology (NIST) in the creation of OSCAL syntax.

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

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

2. FedRAMP Extensions and Allowed Values

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

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

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

As a result, FedRAMP-compliant OSCAL files are a combination of the core OSCAL syntax and extensions defined by FedRAMP. The *Guide to OSCAL-Based FedRAMP Content* describes the concepts behind FedRAMP extensions and allowed values. The extensions related to the System Security Plan (SSP) 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.

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

3. Working with OSCAL Files

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

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

3.1. XML and JSON Formats

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

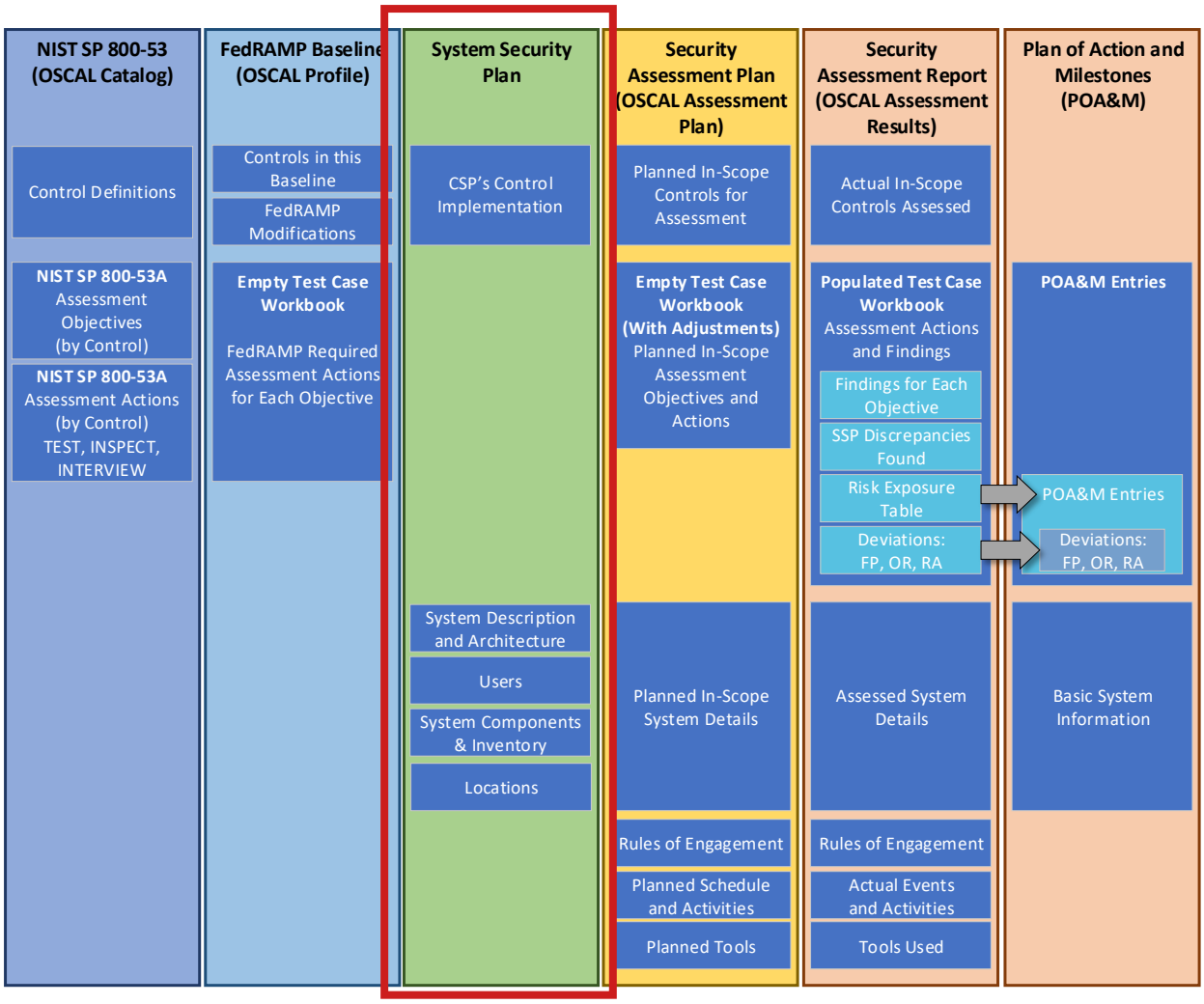
You may submit your SSP to FedRAMP using either format. If necessary, FedRAMP tools will convert the files for processing.

3.2. SSP File Concepts

Unlike the traditional MS Word-based SSP, SAP, and Security Assessment Report (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 NIST control definitions and FedRAMP baseline content that normally appears in the SSP are defined in the FedRAMP profile and simply referenced by the SSP.



Baseline Information is referenced instead of duplicated.

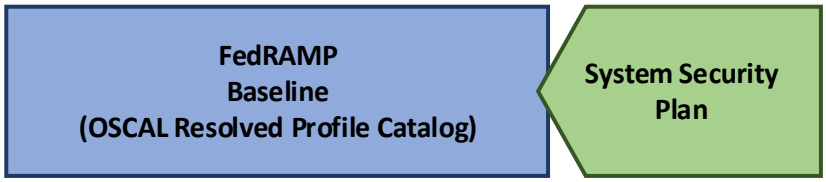
For this reason, an OSCAL-based SSP points to the appropriate OSCAL-based FedRAMP baseline as determined by the system's FIPS-199 impact level. Instead of duplicating control details, the OSCAL-based SSP simply points to the baseline content for information such as control definition statements, FedRAMP-added guidance, parameters, and FedRAMP-required parameter constraints.

3.2.1. Resolved Profile Catalogs

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

Where available, tool developers have the option of following the links from the profile to the catalog as described above or using the resolved profile catalog.

Developers should be aware that at this time, catalogs and profiles remain relatively static. As OSCAL gains wider adoption, there is a risk that profiles and catalogs will become more dynamic, and a resolved profile catalog becomes more likely to be out of date. Early adopters may wish to start with the resolved profile catalog now, and plan to add functionality later for the separate profile and catalog handling later in their product roadmap.



The Resolved Profile Catalog for each FedRAMP Baseline reduces tool processing.

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

3.3. OSCAL-based FedRAMP SSP Template

FedRAMP offers an OSCAL-based SSP 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 shell file. The OSCAL-based FedRAMP SSP Template is available in XML and JSON formats here:

- OSCAL-based FedRAMP SSP Template (JSON Format): https://github.com/GSA/fedramp-automation/raw/master/dist/rev5/content/rev5/templates/ssp/json/FedRAMP-SSP-OSCAL-Template.json
- OSCAL-based FedRAMP SSP Template (XML Format): https://github.com/GSA/fedramp-automation/raw/master/dist/content/rev5/templates/ssp/xml/FedRAMP-SSP-OSCAL-Template.xml

3.4. OSCAL's Minimum File Requirements

Every OSCAL-based FedRAMP SSP file must have a minimum set of required fields/assemblies and must follow the OSCAL SSP core syntax found here:

https://pages.nist.gov/OSCAL/documentation/schema/implementation-layer/ssp

3.5. Importing the FedRAMP Baseline

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

Use the `import-profile` 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.

SSP Import Representation

```
   <import-profile href="path/to/profile.xml" />

- OR -

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

XPath Queries

```
(SSP) URI to Baseline:
  /*/import-profile/@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 SSP file's `back-matter`. Refer to the *Guide to OSCAL-based FedRAMP Content, Section 2.6, Citations, Attachments and Embedded Content in OSCAL Files* for guidance on handling.

SSP Back Matter Representation

```
<back-matter>
    <resource uuid="96445439-6ce1-4e22-beae-aa72cfe173d0">
        <title>FedRAMP Moderate Baseline</title>
        <prop name="type" value="baseline" />
        <!-- Specify the XML or JSON file location. Only one required. -->
        <rlink media-type="application/xml" href="./profile.xml" />
        <rlink media-type="application/json" href="./profile.json" />
    </resource>
</back-matter>
```

XPath Queries

```
(SSP) Referenced OSCAL-based FedRAMP Baseline

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
```

Note: Cloud Service Providers must import FedRAMP profiles or resolved profile catalogs.

3.6. Resolution Resource Prop

FedRAMP will be implementing a separate set of automated SSP validation rules for the rev 5 OSCAL templates. To ensure FedRAMP initiates the appropriate validation rules when processing OSCAL SSPs, SSP 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

```
<system-security-plan>
   <metadata>
      <title>FedRAMP System Security Plan (SSP)</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 SSP (rev 4 or rev 5) this OSCAL
document is for.</p>
         </remarks>
      </resource>

   </back-matter>
</system-security-plan>
```

XPath Queries

```
(SSP) UUID of "resolution-resource":
  /*/metadata/prop[@name="resolution-resource"]/@value

(SSP)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 SSP, FedRAMP will assume the SSP 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.

4. SSP Template to OSCAL Mapping

For SSP-specific content, each main section of the SSP 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 SSP represented in XML format.

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

TOPIC	LOCATION
Title Page	*Guide to OSCAL-based FedRAMP Content, Section 4.1*
Prepared By/For	*Guide to OSCAL-based FedRAMP Content, Section 4.2 - 4.4*
Record of Template Changes	Not Applicable. Instead follow *Guide to OSCAL-based FedRAMP Content, Section 2.3.2, OSCAL Syntax Version*
Revision History	*Guide to OSCAL-based FedRAMP Content, Section 4.5*
How to Contact Us	*Guide to OSCAL-based FedRAMP Content, Section 4.6*
Document Approvers	*Guide to OSCAL-based FedRAMP Content, Section 4.7*
Acronyms and Glossary	*Guide to OSCAL-based FedRAMP Content, Section 4.8*
Laws, Regulations, Standards and Guidance	*Guide to OSCAL-based FedRAMP Content, Section 4.9*
Attachments and Citations	*Guide to OSCAL-based FedRAMP Content, Section 4.10*

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

- Any blue-text instructions found in the SSP template where the instructions are related to the content itself
- Table of Contents
- Introductory and instructive content in section 1, such as references to the NIST SP 800-60 Guide to Mapping Types and the definitions from FIPS Pub 199.
- The control origination definitions are in appendix A of the SSP template; however, please note hybrid and shared are represented in OSCAL by specifying more than one control origination.

The OSCAL syntax in this guide may be used to represent the High, Moderate, and Low FedRAMP SSP Templates. Simply ensure the correct FedRAMP baseline is referenced using the `import-profile` statement.

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

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

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

4.1. System Information

4.1.1. Cloud Service Provider (CSP) Name

The cloud service provider (CSP) must be provided as one of the `party` assemblies within the `metadata`.

```
<system-security-plan>
    <metadata>
        <!-- CSP Name -->
        <party uuid="uuid-of-csp" type="organization">
            <name>Cloud Service Provider (CSP) Name</name>
        </party>
    </metadata>
</system-security-plan>
```

XPath Queries

```
Cloud Service Provider (CSP) Name:
  /*/metadata/party[@uuid='uuid-of-csp']/name
```

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

4.1.2. System Name, Abbreviation, and FedRAMP Unique Identifier

The remainder of the system information is provided in the `system-characteristics` assembly.

The FedRAMP-assigned application number is the unique ID for a FedRAMP system. OSCAL supports several system identifiers, which may be assigned by different organizations.

For this reason, OSCAL requires the `identifier-type` flag be present and have a value that uniquely identifies the issuing organization. FedRAMP requires its value to be "`https://fedramp.gov`" for all FedRAMP-issued application numbers.

Representation

```
<system-security-plan>
    <metadata>
        <!-- CSP Name -->
        <party uuid="uuid-of-csp" type="organization">
            <name>Cloud Service Provider (CSP) Name</name>
        </party>
    </metadata>
    <system-characteristics>
        <!-- System Name & Abbreviation -->
        <system-name>System's Full Name</system-name>
        <system-name-short>System's Short Name or Acronym</system-name-short>
        <!-- FedRAMP Unique Identifier -->
        <system-id identifier-type="http://fedramp.gov">F00000000</system-id>
        <!--  cut -->
    </system-characteristics>
    <!--  cut -->
</system-security-plan>
```

FedRAMP Allowed Value

Required Identifier Type:

- `identifier-type="https://fedramp.gov"`

XPath Queries

```
Information System Name:
  /*/system-characteristics/system-name

Information System Abbreviation:
  /*/system-characteristics/system-name-short

FedRAMP Unique Identifier:
  /*/system-characteristics/system-id[@identifier-type="https://fedramp.gov"]
```

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

4.1.3. Service Model

The core-OSCAL `system-characteristics` assembly has a property for the cloud service model.

Representation

```
<system-security-plan>
    <metadata>
        <!-- CSP Name -->
        <party uuid="uuid-of-csp" type="organization">
            <name>Cloud Service Provider (CSP) Name</name>
        </party>
    </metadata>
    <system-characteristics>
        <!-- System Name & Abbreviation -->
        <system-name>System's Full Name</system-name>
        <system-name-short>System's Short Name or Acronym</system-name-short>
        <!-- FedRAMP Unique Identifier -->
        <system-id identifier-type="http://fedramp.gov">FO0000000</system-id>
        <!-- Service Model -->
        <prop name="cloud-service-model" value="saas">
            <remarks>
                <p>Remarks are required if service model is "other". Optional
otherwise.</p>
            </remarks>
        </prop>

        <!--  cut -->
    </system-characteristics>
    <!--  cut -->
</system-security-plan>
```

NIST Allowed Values

Valid Service Model values:

- `saas`
- `paas`
- `iaas`
- `other`

XPath Queries

```
Service Model:
  /*/system-characteristics/prop[@name="cloud-service-model"]/@value

Remarks on System's Service Model:
  /*/system-characteristics/prop[@name="cloud-service-model"]/remarks/node()
```

NOTE:

- A cloud service provider may define two or more cloud service models for the cloud service offering defined in the system security plan if applicable for customer use (IaaS and PaaS; IaaS and PaaS and SaaS; PaaS and SaaS). Cloud service providers may use a "`cloud-service-model`" `prop` for each applicable cloud service model.
- If the service model is "`other`", the `remarks` field is required. Otherwise, it is optional.

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

FedRAMP Accepted Values

- `name="cloud-deployment-model"`
  Valid: `public-cloud, private-cloud, government-only-cloud, hybrid-cloud, other`

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

4.1.4. Deployment Model

The core-OSCAL `system-characteristics` assembly has a property for the cloud deployment model.

Representation

```
<system-security-plan>
    <metadata>
        <!-- CSP Name -->
        <party uuid="uuid-of-csp" type="organization">
            <name>Cloud Service Provider (CSP) Name</name>
        </party>
    </metadata>
    <system-characteristics>
        <!-- System Name & Abbreviation -->
        <system-name>System's Full Name</system-name>
        <system-name-short>System's Short Name or Acronym</system-name-short>
        <!-- FedRAMP Unique Identifier -->
        <system-id identifier-type="http://fedramp.gov">F00000000</system-id>
        <!-- Service Model -->
        <prop name="cloud-service-model" value="saas">
            <remarks>
                <p>Remarks are required if service model is "other". Optional
otherwise.</p>
            </remarks>
        </prop>
        <!-- Deployment Model -->
        <prop name="cloud-deployment-model" value="public-cloud">
            <remarks>
                <p>Remarks are required if deployment model is "hybrid". Optional
otherwise.</p>
            </remarks>
        </prop>
        <!--  cut -->
    </system-characteristics>
    <!--  cut -->
</system-security-plan>
```

XPath Queries

```
Deployment Model:
  /*/system-characteristics/prop[@name="cloud-deployment-model"]/@value

Remarks on System's Deployment Model:
  /*/system-characteristics/prop[@name="cloud-deployment-model"]/remarks/node()
```

NOTE:

- A cloud service provider may define one and only one cloud deployment model in the system security plan for a cloud service offering.
- OSCAL 1.0.0 permits `a cloud-deployment-model` of value `community-cloud`, but FedRAMP does not permit such a deployment model for cloud service offerings and is not permitted for a FedRAMP OSCAL-based system security plan.
- If the deployment model is "`hybrid`", the `remarks` field is required. Otherwise, it is optional.

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

4.1.5. Digital Identity Level (DIL) Determination

The digital identity level identified in Table 1.0 is the same as the level in Attachment 3. It is expressed through the following core OSCAL properties.

Representation

```
<system-security-plan>
    <metadata>
        <!-- cut CSP Name -->
    </metadata>
    <system-characteristics>
        <!-- System Name & Abbreviation -->
        <system-name>System's Full Name</system-name>
        <system-name-short>System's Short Name or Acronym</system-name-short>
        <!-- FedRAMP Unique Identifier -->
        <system-id identifier-type="http://fedramp.gov">F00000000</system-id>
        <!-- cut Service Model -->
        <!-- cut Deployment Model -->

        <!-- DIL Determination -->
        <prop name="identity-assurance-level" value="1"/>
        <prop name="authenticator-assurance-level" value="1"/>
        <prop name="federation-assurance-level" value="1"/>

        <!--  cut -->
    </system-characteristics>
    <!--  cut -->
</system-security-plan>
```

NIST Allowed Values

Valid IAL, AAL, and FAL values (as defined by NIST 800-63):

- 1
- 2
- 3

XPath Queries

```
Identity Assurance Level:
  /*/system-characteristics/prop[@name="identity-assurance-level"]/@value

Authenticator Assurance Level:
  /*/system-characteristics/prop[@name="authenticator-assurance-level"]/@value

Federation Assurance Level:
  /*/system-characteristics/prop[@name="federation-assurance-level"]/@value
```

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

4.1.6. System Sensitivity Level

The privacy system designation in Table 1.0 is the same as in Attachment 4. It is expressed through the following core OSCAL property.

Representation

```
<system-security-plan>
    <metadata>
        <!-- cut CSP Name -->
    </metadata>
    <system-characteristics>
        <!-- System Name & Abbreviation -->
        <system-name>System's Full Name</system-name>
        <system-name-short>System's Short Name or Acronym</system-name-short>
        <!-- FedRAMP Unique Identifier -->
        <system-id identifier-type="http://fedramp.gov">F00000000</system-id>
        <!-- cut Service Model -->
        <!-- cut Deployment Model -->
        <!-- cut DIL Determination -->

        <!-- FIPS PUB 199 Level (SSP Attachment 10) -->
        <security-sensitivity-level>fips-199-moderate</security-sensitivity-level>

        <!--  cut -->
    </system-characteristics>
    <!--  cut -->
</system-security-plan>
```

OSCAL Allowed Values

Valid values for `security-sensitivity-level`:

- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

XPath Queries

```
System Sensitivity Level:
  /*/system-characteristics/security-sensitivity-level
```

NOTES:

- The identified System Sensitivity Level governs which FedRAMP baseline applies. See Appendix A for more information about importing the appropriate FedRAMP baseline.

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

4.1.7. System Status

Representation

```
<system-security-plan>
    <metadata>
        <!-- cut CSP Name -->
    </metadata>
    <system-characteristics>
        <!-- System Name & Abbreviation -->
        <system-name>System's Full Name</system-name>
        <system-name-short>System's Short Name or Acronym</system-name-short>
        <!-- FedRAMP Unique Identifier -->
        <system-id identifier-type="http://fedramp.gov/ns/oscal">F00000000</system-id>
        <!-- cut Service Model -->
        <!-- cut Deployment Model -->
        <!-- cut DIL Determination -->

        <!-- FIPS PUB 199 Level (SSP Attachment 10) -->
        <security-sensitivity-level>fips-199-moderate</security-sensitivity-level>
        <!-- Fully Operational as of -->
        <status state="operational">
            <remarks>
                <p>Remarks are optional if status/state is "operational".</p>
                <p>Remarks are required otherwise.</p>
            </remarks>
        </status>
        <prop ns="https://fedramp.gov/ns/oscal" name="fully-operational-date"
              value="mm/dd/yyyy"/>

        <!--  cut -->
    </system-characteristics>
    <!--  cut -->
</system-security-plan>
```

NIST Allowed Values

FedRAMP only accepts those in bold:

- **operational**
- under-development
- **under-major-modification**
- disposition
- **other**

XPath Queries

```
System's Operational Status:
  /*/system-characteristics/status/@state

Remarks on System's Operational Status:
  /*/system-characteristics/status/remarks/node()

Fully Operational As Of Date:
  /*/system-characteristics/prop[@name="fully-operational-
  date"][@ns="https://fedramp.gov/ns/oscal"]/@value
```

NOTE:

- If the status is "`other`", the `remarks` field is required. Otherwise, it is optional.
- While `under-development`, and `disposition` are valid OSCAL values, systems with either of these operational status values are not eligible for a FedRAMP Authorization.

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

4.1.8. System Functionality

Representation

```
<system-security-plan>
    <metadata>
        <!-- cut CSP Name -->
    </metadata>
    <system-characteristics>
        <!-- System Name & Abbreviation -->
        <system-name>System's Full Name</system-name>
        <system-name-short>System's Short Name or Acronym</system-name-short>
        <!-- FedRAMP Unique Identifier -->
        <system-id identifier-type="http://fedramp.gov/ns/oscal">F00000000</system-id>
        <!-- cut Service Model -->
        <!-- cut Deployment Model -->
        <!-- cut DIL Determination -->

        <!-- FIPS PUB 199 Level (SSP Attachment 10) -->
        <security-sensitivity-level>fips-199-moderate</security-sensitivity-level>
        <!-- cut Fully Operational as of -->

        <!-- system functionality -->
        <description>
            <p>Describe the purpose and functions of this system here.</p>
            <!-- list of services/features in scope -->
            <!-- (use paragraph, list item, or table) -->
        </description>

    </system-characteristics>
    <!--  cut -->
</system-security-plan>
```

XPath Queries

```
System Function or Purpose: First paragraph in description
  /*/system-characteristics/description/node()
```

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:https://pages.nist.gov/OSCAL/reference/datatypes/#markup-data-types

Table 4.1 <Insert CSO Name> Owner

System Owner Information	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter Email Address>

NOTES ON ADDRESSES

Preferred Approach: When multiple parties share the same address, such as multiple staff members at a company HQ, define the location once as a `location` assembly, then use the `location-uuid` field within each `party` assembly to identify the location of that individual or team.

Alternate Approach: If the address is unique to this individual, it may be included in the `party` assembly itself.

Hybrid Approach: It is possible to include both a `location-uuid` and an `address` assembly within a `party` assembly. This may be used where multiple staff are in the same building but have different office numbers or mail stops. Use the `location-uuid` to identify the shared building, and only include a single `addr-line` field within the party's `address` assembly.

A tool developer may elect to always create a location assembly, even when only used once; however, tools must recognize and handle all of the approaches above when processing OSCAL files.

4.2. Information System Owner

A role with an ID value of "`system-owner`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the System Owner's information.

Representation

```
<metadata>
    <!-- cut -->
    <role id="system-owner"><!-- cut --></role>
    <location uuid="uuid-of-hq-location">
        <title>CSP HQ</title>
        <address type="work">
            <addr-line>1234 Some Street</addr-line>
            <city>Haven</city>
            <state>ME</state>
            <postal-code>00000</postal-code>
        </address>
    </location>
    <party uuid="uuid-of-csp" type="organization">
        <name>Cloud Service Provider (CSP) Name</name>
    </party>
    <party uuid="uuid-of-person-1" type="person">
        <name>[SAMPLE]Person Name 1</name>
        <prop name="job-title" value="Individual's Title"/>
            <prop name="mail-stop" value="A-1"/>
                <email-address>name@example.com</email-address>
                <telephone-number>202-000-0000</telephone-number>
                <location-uuid>uuid-of-hq-location</location-uuid>
                <member-of-organization>uuid-of-csp</member-of-organization>
    </party>
    <responsible-party role-id="system-owner">
        <party-uuid>uuid-of-person-1</party-uuid>
    </responsible-party>
</metadata>
```

NIST Allowed Value

Required role ID:

- `system-owner`

XPath Queries

```
System Owner's Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-owner"]/
  party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

System Owner's Address:
  /*/metadata/location[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="system-owner"]/party-uuid]]/location-uuid]/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

System Owner's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-owner"]/
  party-uuid]]/prop[@name='job-title']/@value

Company/Organization:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="system-owner"]/party-uuid]]/member-of-organization]/name
```

NOTE:

If no country is provided, FedRAMP tools will assume a US address.

FedRAMP JAB P-ATO Authorization Representation

```
<metadata>
    <!-- cut -->
    <role id="authorizing-official">
        <title>Authorizing Official</title>
        <desc>The government executive(s) who authorize this system.</desc>
    </role>
    <!-- cut -->
    <party uuid="uuid-of-fedramp-jab" type="organization">
        <name>FedRAMP: Joint Authorization Board</name>
        <short-name>FedRAMP JAB</short-name>
    </party>
    <!-- cut -->
    <responsible-party role-id="authorizing-official">
        <party-uuid>uuid-of-fedramp-jab</party-uuid>
    </responsible-party>
</metadata>
<!-- import -->
<system-characteristics>
    <!-- description -->
    <prop name="authorization-type"
          ns="https://fedramp.gov/ns/oscal">fedramp-jab</prop>
    <!-- prop -->
</system-characteristics>
```

JAB XPath Queries

```
Authorizing Official's Name:
  //metadata/party[@uuid=[//metadata/responsible-party[@role-id="authorizing-
  official"]/party-uuid]]/name
```

FedRAMP Extension:

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

- name="authorization-type"

FedRAMP Allowed Values

- fedramp-jab
- fedramp-agency
- fedramp-li-saas

NIST Allowed Value

Required Role ID:

- authorizing-official

4.3. Federal Authorizing Officials

A role with an ID value of "authorizing-official" is required. Use the responsible-party assembly to associate this role with the party assembly containing the Authorizing Official's information.

FedRAMP Agency Authorization Representation

```
<metadata>
    <role id="authorizing-official">
        <title>Authorizing Official</title>
    </role>
    <party uuid="uuid-of-agency" type="organization">
        <name>Agency Name</name>
    </party>
    <party uuid="uuid-of-person-6" type="person">
        <name>[SAMPLE]Person Name 6</name>
        <prop name="job-title" value="Individual's Title"/>
            <email-address>name@example.com</email-address>
            <telephone-number>202-000-0000</telephone-number>
            <member-of-organization>uuid-of-agency</member-of-organization>
    </party>
    <responsible-party role-id="authorizing-official">
        <party-uuid>uuid-of-person-6</party-uuid>
    </responsible-party>
</metadata>
<!-- import -->
<system-characteristics>
    <!-- description -->
    <prop name="authorization-type"
          ns="https://fedramp.gov/ns/oscal"
          value="fedramp-agency" />
    <!-- prop -->
</system-characteristics>
```

Authorization Type XPath Query

```
FedRAMP Authorization Type:
  /*/system-characteristics/prop[@name="authorization-type"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value
```

FedRAMP Agency and LI-SaaS XPath Queries

```
Authorizing Official's Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="authorizing-official"]/party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

Authorizing Official's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party [@role-
  id="authorizing-official"]/party-uuid]]/prop[@name='job-title']

Authorizing Official's Agency:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="authorizing-official"]/party-uuid]]/member-of-organization]/name
```

NOTE:

If the authorization-type field is "fedramp-jab", the responsible-party/party-uuid field must be the uuid value for the FedRAMP JAB.

FedRAMP JAB P-ATO Authorization Representation

```
<metadata>
    <!-- cut -->
    <role id="authorizing-official">
        <title>Authorizing Official</title>
        <desc>The government executive(s) who authorize this system.</desc>
    </role>
    <!-- cut -->
    <party uuid="uuid-of-fedramp-jab" type="organization">
        <name>FedRAMP: Joint Authorization Board</name>
        <short-name>FedRAMP JAB</short-name>
    </party>
    <!-- cut -->
    <responsible-party role-id="authorizing-official">
        <party-uuid>uuid-of-fedramp-jab</party-uuid>
    </responsible-party>
</metadata>
<!-- import -->
<system-characteristics>
    <!-- description -->
    <prop name="authorization-type"
          ns="https://fedramp.gov/ns/oscal">fedramp-jab</prop>
    <!-- prop -->
</system-characteristics>
```

JAB XPath Queries

```
Authorizing Official's Name:
  //metadata/party[@uuid=[//metadata/responsible-party[@role-id="authorizing-
  official"]/party-uuid]]/name
```

NIST Allowed Value

Required Role ID:

- `authorizing-official`

FEDRAMP _____ BASELINE SYSTEM SECURITY PLAN (SSP) TEMPLATE

CSP|CSO| *Version Number, Date*

ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officer (ISSO), or equivalent, identified below, has been ***appointed in writing*** and is deemed to have significant cyber security and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 5.1 <Insert CSP Name> ISSO (or Equivalent) Point of Contact

ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

NOTES ON ADDRESSES

Preferred Approach: When multiple parties share the same address, such as multiple staff members at a company HQ, define the location once as a `location` assembly, then use the `location-uuid` field within each `party` assembly to identify the location of that individual or team.

Alternate Approach: If the address is unique to this individual, it may be included in the `party` assembly itself.

Hybrid Approach: It is possible to include both a `location-uuid` and an `address` assembly within a `party` assembly. This may be used where multiple staff are in the same building but have different office numbers or mail stops. Use the `location-uuid` to identify the shared building, and only include a single `addr-line` field within the party's `address` assembly.

A tool developer may elect to always create a location assembly, even when only used once; however, tools must recognize and handle all of the approaches above when processing OSCAL files.

4.4. Assignment of Security Responsibilities

A role with an ID value of "`information-system-security-officer`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the Information System Security Officer's information.

Table 6-1 Representation

```
<metadata>
    <!-- cut -->
    <role id="information-system-security-officer"><!-- cut -->
        <title>System Information System Security Officer (or Equivalent)</title>
    </role>
    <location uuid="uuid-of-hq-location">
        <title>CSP HQ</title>
        <address type="work">
            <addr-line>1234 Some Street</addr-line>
            <city>Haven</city>
            <state>ME</state>
            <postal-code>00000</postal-code>
        </address>
    </location>
    <party uuid="uuid-of-csp" type="organization">
        <name>Cloud Service Provider (CSP) Name</name>
    </party>
    <party uuid="uuid-of-person-10" type="person">
        <name>[SAMPLE]Person Name 10</name>
        <prop name="job-title" value="Individual's Title"/>
        <email-address>name@org.domain</email-address>
        <telephone-number>202-000-0000</telephone-number>
        <location-uuid>uuid-of-hq-location</location-uuid>
        <member-of-organization>uuid-of-csp</member-of-organization>
    </party>
    <!-- repeat party assembly for each person -->
    <responsible-party role-id="system-poc-technical">
        <party-uuid>uuid-of-person-7</party-uuid>
    </responsible-party>
</metadata>
```

NIST Allowed Value

Required Role ID:

- `information-system-security-officer`

XPath Queries

```
ISSO POC Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="information-system-
  security-officer"]/party-uuid]]/name
NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.
ISSO POC's Address:
  /*/metadata/location[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party [@role-
  id="information-system-security-officer"]/party-uuid]]/location-uuid]/address/addr-line
NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.
ISSO POC's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="information-system-
  security-officer"]/party-uuid]]/prop[@name='job-title']
Company/Organization:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="information-system-security-officer"]/party-uuid]]/member-of-
  organization]/name
```

Table 6.1 Leveraged FedRAMP Authorized Services

#	CSP/CSO Name (Name on FedRAMP Marketplace)	CSO Service (Names of services and features - services from a single CSO can be all listed in one cell)	Authorization Type (JAB or Agency) and FedRAMP Package ID #	Nature of Agreement	Impact Level (High, Moderate, Low, LI-SaaS)	Data Types	Authorized Users/Authentication

IMPORTANT FOR LEVERAGED SYSTEMS:

While a leveraged system has no need to represent content here, its SSP must include special inheritance and responsibility information in the individual controls. See *Section 6.4.8, Response: Identifying Inheritable Controls and Customer Responsibilities* for more information.

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

The `date-authorized` field is string type *date*, which requires a four-digit year, a dash, a two-digit month, a dash, a two-digit day, and an optional time zone offset. (`yyyy-mm-dd` or `yyyy-mm-dd-05:00`)

For more information, visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#date

Additional information is required within each control. See *Section 6.4.9, Leveraged Authorization Response: Inheriting Controls, Satisfying Responsibilities* for more information.

4.5. Leveraged FedRAMP-authorized Services

If this system is leveraging the authorization of one or more systems, such as a SaaS running on an IaaS, each leveraged system must be represented within the `system-implementation` assembly. There must be one `leveraged-authorization` assembly and one matching `component` assembly for each leveraged authorization.

The `leveraged-authorization` assembly includes the leveraged system's name, point of contact (POC), and authorization date. The `component` assembly must be linked to the `leveraged-authorization` assembly using a property (`prop`) field with the name `leveraged-authorization-uuid` and the UUID value of its associated `leveraged-authorization` assembly. The `component` assembly enables controls to reference it with the `by-component` responses described in *Section 6.4, Control Implementation Descriptions*. The `implementation-point` property value must be set to "`external`".

If the leveraged system owner provides a UUID for their system, such as in an OSCAL-based Inheritance and Responsibility document (similar to a CRM), it should be provided as the `inherited-uuid` property value.

Representation

```
<metadata>
    <!—CSP name -->
    <party uuid="uuid-value">
        <name>Example IaaS Provider</name>
        <short-name>E.I.P.</short-name>
    </party>
</metadata>
<!-- cut import-profile, system-characteristics -->
<system-implementation>
    <leveraged-authorization uuid="uuid-value" >
        <title>Name of Underlying System</title>
        <!—FedRAMP Package ID -->
        <prop name="leveraged-system-identifier"
            ns="https://fedramp.gov/ns/oscal"
            value="Package ID value" />
        <prop ns="https://fedramp.gov/ns/oscal" name="authorization-type"
              value="fedramp-agency"/>
        <prop ns="https://fedramp.gov/ns/oscal" name="impact-level" value="moderate"/>
        <link href="//path/to/leveraged system legacy crm.xslt" />
        <link href="//path/to/leveraged system responsibility and inheritance.xml" />
        <party-uuid>uuid-of-leveraged-system-poc</party-uuid>
        <date-authorized>2015-01-01</date-authorized>
    </leveraged-authorization>
    <!-- CSO name & service description -->
    <component uuid="uuid-of-leveraged-system" type="leveraged-system">
        <title>Name of Leveraged System</title>
        <description>
            <p>Briefly describe leveraged system.</p>
        </description>
        <prop name="leveraged-authorization-uuid"
              value="5a9c98ab-8e5e-433d-a7bd-515c07cd1497" />
        <prop name="inherited-uuid" value="11111111-0000-4000-9001-000000000001" />
        <prop name="implementation-point" value="external"/>
        <!—FedRAMP prop extensions for table 6.1 columns -->
        <status state="operational"/>
    </component>
</system-implementation>
```

The `title` field must match an existing FedRAMP authorized Cloud_Service_Provider_Package property value.

A `leveraged-system-identifier` property must be provided within each `leveraged-authorization` field. The value of this property must be from the same Cloud Service Provider as identified in the `title` field.

Table 6.1 Leveraged FedRAMP Authorized Services

#	CSP/CSO Name (Name on FedRAMP Marketplace)	CSO Service (Names of services and features - services from a single CSO can be all listed in one cell)	Authorization Type (JAB or Agency) and FedRAMP Package ID #	Nature of Agreement	Impact Level (High, Moderate, Low, LI-SaaS)	Data Types	Authorized Users/Authentication

IMPORTANT FOR LEVERAGED SYSTEMS:

While a leveraged system has no need to represent content here, its SSP must include special inheritance and responsibility information in the individual controls. See *Section 6.4.8, Response: Identifying Inheritable Controls and Customer Responsibilities* for more information.

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:

https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

XPath Queries

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

Name of first leveraged system:
```
/*/system-implementation/leveraged-authorization[1]/title
```

Name of first leveraged system CSO service (component):
```
(//*/component/prop[@name="leveraged-authorization-uuid" and @value="uuid-of-leveraged-system"]/parent::component/title)[1]
```

Description of first leveraged system CSO service (component):
```
(//*/component/prop[@name="leveraged-authorization-uuid" and @value="uuid-of-leveraged-system"]/parent::component/description)[1]
```

Authorization type of first leveraged system:
```
/system-security-plan/system-implementation[1]/leveraged-authorization[1]/prop[@ns="https://fedramp.gov/ns/oscal" and @name="authorization-type"]/@value
```

FedRAMP package ID# of the first leveraged system:
```
/system-security-plan/system-implementation[1]/leveraged-authorization[1]/prop[@ns="https://fedramp.gov/ns/oscal" and @name="leveraged-system-identifier"]/@value
```

Nature of Agreement for first leveraged system:
```
(//*/component/prop[@name="leveraged-authorization-uuid" and @value="uuid-of-leveraged-system"]/parent::component/prop[@ns="https://fedramp.gov/ns/oscal" and @name="nature-of-agreement"]/@value)[1]
```

FedRAMP impact level of the first leveraged system:
```
/system-security-plan/system-implementation[1]/leveraged-authorization[1]/prop[@ns="https://fedramp.gov/ns/oscal" and @name="impact-level"]/@value
```

Data Types transmitted to, stored or processed by the first leveraged system CSO:
```
(//*/component/prop[@name="leveraged-authorization-uuid" and @value="uuid-of-leveraged-system"]/parent::component/prop[@ns="https://fedramp.gov/ns/oscal" and @name="interconnection-data-type"]/@value)
```

Authorized Users of the first leveraged system CSO:
```
//system-security-plan/system-implementation/user[@uuid="uuid-of-user"]
```

Corresponding Access Level:
```
//system-security-plan/system-implementation/user[@uuid="uuid-of-user"]/prop @name="privilege-level"]/@value
```

Corresponding Authentication method:
```
//system-security-plan/system-implementation/user[@uuid="uuid-of-user"]/prop[@ns="https://fedramp.gov/ns/oscal" and @name="authentication-method"]/@value
```

Table 7.1 External Systems/Services, Interconnections, APIs, and CLIs Without FedRAMP Authorizations

# (either 1, 2, or 3)**	System/ Service/ API/CLI Name (Non-FedRAMP Cloud Services)	Connection Details	Nature of Agreement	Still Supported? Y or N	Data Types	Data Categorization	Authorized Users/ Authentication	Other Compliance Programs	Description	Hosting Environment	Risk/Impact/ Mitigation

***1- Non-FedRAMP Authorized Cloud Services, 2- Corporate Shared Services, 3- Update Services for In-Boundary Software/Services*

FedRAMP Extensions & Allowed Values

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

- `name="service-processor"`
- `name="information`
- `name="port"`
- `name="circuit"`

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

- `name="connection-security"`
  - **Valid**: ipsec, vpn, ssl, certificate, secure-file-transfer, other

NIST Allowed Values

Required ICA Role IDs:

- `isa-poc-remote`
- `isa-poc-local`
- `isa-authorizing-official-remote`
- `isa-authorizing-official-local`

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.6. External Systems and Services Not Having FedRAMP Authorization

Representation

```
<!-- list any external connections as components in the system-characteristics -->
    <component uuid="uuid-value" type="interconnection">
        <title>[EXAMPLE]External System / Service Name</title>
        <description>
            <p>Briefly describe the interconnection details.</p>
        </description>
        <!—Props for table 7.1 columns -->
        <prop ns="https://fedramp.gov/ns/oscal" name="service-processor"
              value="[SAMPLE] Telco Name"/>
         <prop ns="https://fedramp.gov/ns/oscal" name="interconnection-type" value="1" />
         <prop name="direction" value="incoming"/>
         <prop name="direction" value="outgoing"/>
         <prop ns="https://fedramp.gov/ns/oscal" name="nature-of-agreement"
               value="contract" />
         <prop ns="https://fedramp.gov/ns/oscal" name="still-supported" value="yes" />
         <prop ns="https://fedramp.gov/ns/oscal" class="fedramp"
               name="interconnection-data-type" value="C.3.5.1" />
         <prop ns="https://fedramp.gov/ns/oscal" class="fedramp"
               name="interconnection-data-type" value="C.3.5.8" />
         <prop ns="https://fedramp.gov/ns/oscal" class="C.3.5.1"
               name="interconnection-data-categorization" value="low" />
         <prop ns="https://fedramp.gov/ns/oscal" class="C.3.5.8"
               name="interconnection-data-categorization" value="moderate" />
         <prop ns="https://fedramp.gov/ns/oscal" name="authorized-users"
               value="SecOps engineers" />
         <prop ns="https://fedramp.gov/ns/oscal" class="fedramp"
               name="interconnection-compliance" value="PCI SOC 2" />
         <prop ns="https://fedramp.gov/ns/oscal" class="fedramp"
               name="interconnection-compliance" value="ISO/IEC 27001" />
         <prop ns="https://fedramp.gov/ns/oscal" name="interconnection-hosting-environment"
               value="PaaS" />
         <prop ns="https://fedramp.gov/ns/oscal" name="interconnection-risk" value="None" />
         <prop name="isa-title" value="system interconnection agreement"/>
         <prop name="isa-date" value="2023-01-01T00:00:00Z"/>
         <prop name="ipv4-address" class="local" value="10.1.1.1"/>
         <prop name="ipv4-address" class="remote" value="10.2.2.2"/>
         <prop name="ipv6-address" value="::ffff:10.2.2.2"/>
         <prop ns="https://fedramp.gov/ns/oscal" name="information"
               value="Describe the information being transmitted."/>
         <prop ns="https://fedramp.gov/ns/oscal" name="port" class="remote" value="80"/>
         <prop ns="https://fedramp.gov/ns/oscal" name="interconnection-security"
               value="ipsec">
          <!-- cut ports, protocols -->
        <link href="#uuid-of-ICA-resource-in-back-matter" rel="isa-agreement" />
        <!-- cut repeat responsible-party assembly for each required ICA role id -->
    </component>
<!-- cut …. -->
<back-matter>
    <resource uuid="uuid-value">
        <title>[SAMPLE]Interconnection Security Agreement Title</title>
        <prop name="version" value="Document Version"/>
        <rlink href="./documents/ISAs/ISA-1.docx"/>
        <citation><!-- cut --></citation>
    </resource>
    <!-- repeat citation assembly for each ICA -->
</back-matter>
```

Table 7.1 External Systems/Services, Interconnections, APIs, and CLIs Without FedRAMP Authorizations

# (either 1, 2, or 3)**	System/ Service/ API/CLI Name (Non-FedRAMP Cloud Services)	Connection Details	Nature of Agreement	Still Supported? Y or N	Data Types	Data Categorization	Authorized Users/ Authentication	Other Compliance Programs	Description	Hosting Environment	Risk/Impact/ Mitigation

***1- Non-FedRAMP Authorized Cloud Services, 2- Corporate Shared Services, 3- Update Services for In-Boundary Software/Services*

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

Queries are for the Interconnection Security Agreement (ISA)'s remote POC and authorizing official (AO) information. To obtain the ISA's local POC and AO information:

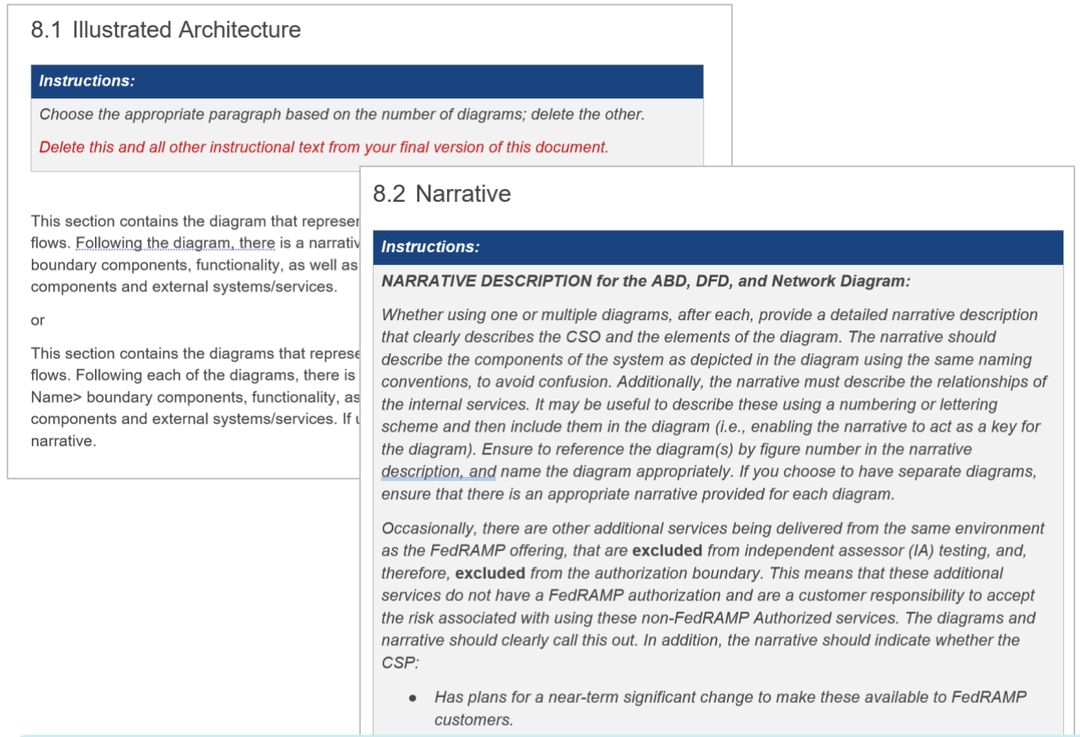
```
Replace "isa-poc-remote" with "isa-poc-local"
Replace "[isa-authorizing-official-remote" with "isa-authorizing-official-local"
```

4.7 External System and Services (Queries)

XPath Queries

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

```
Interconnection # for first external system:
  /*/system-implementation/component[@type='interconnection'][1]/
  prop[@ns="https://fedramp.gov/ns/oscal" and @name="interconnection-type"]/@value

System/Service/API/CLI Name:
  /*/system-implementation/component[@type='interconnection']/title

Connection Details:
  /*/system-
  implementation/component[@type='interconnection'][1]/prop[@name="direction"]/@value

Nature of Agreement for first external system:
  /*/system-implementation/component[@type='interconnection'][1]/
  prop[@ns="https://fedramp.gov/ns/oscal" and @name="nature-of-agreement"]/@value

Still Supported (Y/N):
  /*/system-implementation/component[@type='interconnection'][1]/
  prop[@ns="https://fedramp.gov/ns/oscal" and @name="still-supported"]/@value

Data Types:
  /*/system-
  implementation/component[@type='interconnection'][1]/prop[@ns="https://fedramp.gov/ns/
  oscal" and @name="interconnection-data-type"]/@value

Data Categorization:
  /*/system-
  implementation/component[@type='interconnection'][1]/prop[@ns="https://fedramp.gov/ns/
  oscal" and @name="interconnection-data-categorization"]/@value

Authorized Users:
  //system-security-plan/system-implementation/user[@uuid="uuid-of-user"]

Corresponding Access Level:
  //system-security-plan/system-implementation/user[@uuid="uuid-of-user"]/prop
  @name="privilege-level"]/@value

Other Compliance Programs:
  /*/system-
  implementation/component[@type='interconnection'][1]/prop[@ns="https://fedramp.gov/ns/
  oscal" and @name="interconnection-compliance"]/@value

Description:

/*/system-implementation/component[@type='interconnection'][1]/description

Hosting Environment:
  /*/system-
  implementation/component[@type='interconnection'][1]/prop[@ns="https://fedramp.gov/ns/oscal"
  and @name="interconnection-hosting-environment"]/@value

Risk/Impact/Mitigation:
  /*/system-
  implementation/component[@type='interconnection'][1]/prop[@ns="https://fedramp.gov/ns/oscal"
  and @name="interconnection-risk"]/@value
```



8.1 Illustrated Architecture

Instructions:

Choose the appropriate paragraph based on the number of diagrams; delete the other.

Delete this and all other instructional text from your final version of this document.

This section contains the diagram that represer
flows. Following the diagram, there is a narrativ
boundary components, functionality, as well as
components and external systems/services.

or

This section contains the diagrams that represe
flows. Following each of the diagrams, there is
Name> boundary components, functionality, as
components and external systems/services. If
narrative.

8.2 Narrative

Instructions:

NARRATIVE DESCRIPTION for the ABD, DFD, and Network Diagram:

Whether using one or multiple diagrams, after each, provide a detailed narrative description that clearly describes the CSO and the elements of the diagram. The narrative should describe the components of the system as depicted in the diagram using the same naming conventions, to avoid confusion. Additionally, the narrative must describe the relationships of the internal services. It may be useful to describe these using a numbering or lettering scheme and then include them in the diagram (i.e., enabling the narrative to act as a key for the diagram). Ensure to reference the diagram(s) by figure number in the narrative description, and name the diagram appropriately. If you choose to have separate diagrams, ensure that there is an appropriate narrative provided for each diagram.

Occasionally, there are other additional services being delivered from the same environment as the FedRAMP offering, that are **excluded** *from independent assessor (IA) testing, and, therefore,* **excluded** *from the authorization boundary. This means that these additional services do not have a FedRAMP authorization and are a customer responsibility to accept the risk associated with using these non-FedRAMP Authorized services. The diagrams and narrative should clearly call this out. In addition, the narrative should indicate whether the CSP:*

- *Has plans for a near-term significant change to make these available to FedRAMP customers.*

In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter/resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/back-matter/resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*.
These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

4.8 Illustrated Architecture and Narratives

4.8.1Authorization Boundary

The OSCAL approach to this type of diagram is to treat the image data as either a linked or base64-encoded `resource` in the `back-matter` section of the OSCAL file, then reference the diagram using the `link` field.

Representation

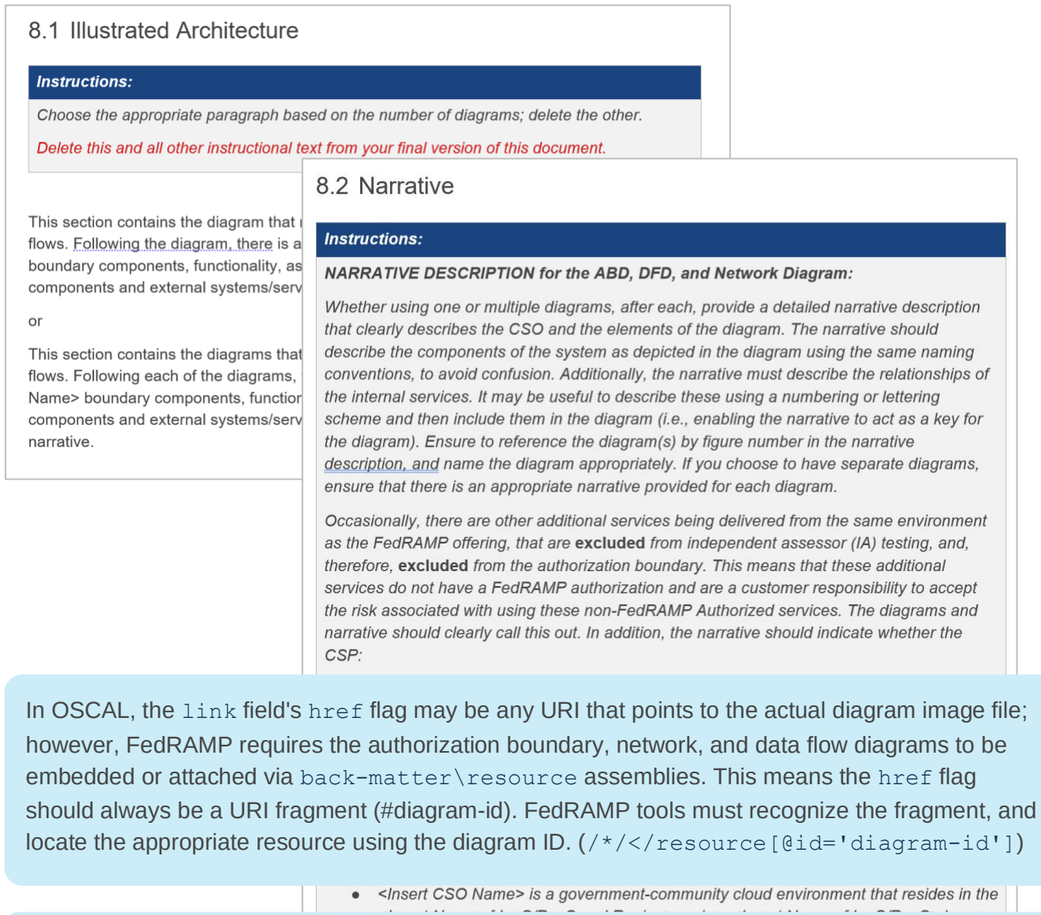
```
<system-characteristics>
    <!-- leveraged-authorization -->
    <authorization-boundary>
        <!-- 8.2 Narrative (Boundary) -->
        <description>
            <p>A holistic, top-level explanation of the FedRAMP authorization boundary.</p>
        </description>
        <!-- 8.1 Illustrated Architecture (Boundary) -->
        <diagram uuid="uuid-value">
            <description><p>A diagram-specific explanation.</p></description>
            <link href="#uuid-of-boundary-diagram-1" rel="diagram" />
            <caption>Authorization Boundary Diagram</caption>
        </diagram>
        <!-- repeat diagram assembly for each additional boundary diagram -->
    </authorization-boundary>
    <!-- network-architecture -->
</system-characteristics>

<!-- cut -->

<back-matter>
    <resource uuid="uuid-of-boundary-diagram-1">
        <description><p>The primary authorization boundary diagram.</p></description>
        <base64 filename="architecture-main.png" media-type="image/png">00000000</base64>
    </resource>
</back-matter>
```

XPath Queries

```
Overall Description:
  /*/system-characteristics/authorization-boundary/description/node()

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/authorization-boundary/diagram)

Link to First Diagram:
  /*/system-characteristics/authorization-boundary/diagram[1]/link/@href
```

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

```
If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@uuid="uuid-of-boundary-diagram"]/base64
  OR:
  /*/back-matter/resource[@uuid="uuid-of-boundary-diagram-1"]/rlink/@href

Diagram-specific Description:
  /*/system-characteristics/authorization-boundary/diagram[1]/description/node()
```



8.1 Illustrated Architecture

Instructions:

Choose the appropriate paragraph based on the number of diagrams; delete the other.

Delete this and all other instructional text from your final version of this document.

This section contains the diagram that
flows. Following the diagram, there is a
boundary components, functionality, as
components and external systems/serv

or

This section contains the diagrams that
flows. Following each of the diagrams,
Name> boundary components, functior
components and external systems/serv
narrative.

8.2 Narrative

Instructions:

NARRATIVE DESCRIPTION for the ABD, DFD, and Network Diagram:

Whether using one or multiple diagrams, after each, provide a detailed narrative description that clearly describes the CSO and the elements of the diagram. The narrative should describe the components of the system as depicted in the diagram using the same naming conventions, to avoid confusion. Additionally, the narrative must describe the relationships of the internal services. It may be useful to describe these using a numbering or lettering scheme and then include them in the diagram (i.e., enabling the narrative to act as a key for the diagram). Ensure to reference the diagram(s) by figure number in the narrative description, and name the diagram appropriately. If you choose to have separate diagrams, ensure that there is an appropriate narrative provided for each diagram.

Occasionally, there are other additional services being delivered from the same environment as the FedRAMP offering, that are **excluded** *from independent assessor (IA) testing, and, therefore,* **excluded** *from the authorization boundary. This means that these additional services do not have a FedRAMP authorization and are a customer responsibility to accept the risk associated with using these non-FedRAMP Authorized services. The diagrams and narrative should clearly call this out. In addition, the narrative should indicate whether the CSP:*

- *<Insert CSO Name> is a government-community cloud environment that resides in the*

In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter\resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/</resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

4.8.2 Network Architecture

Representation

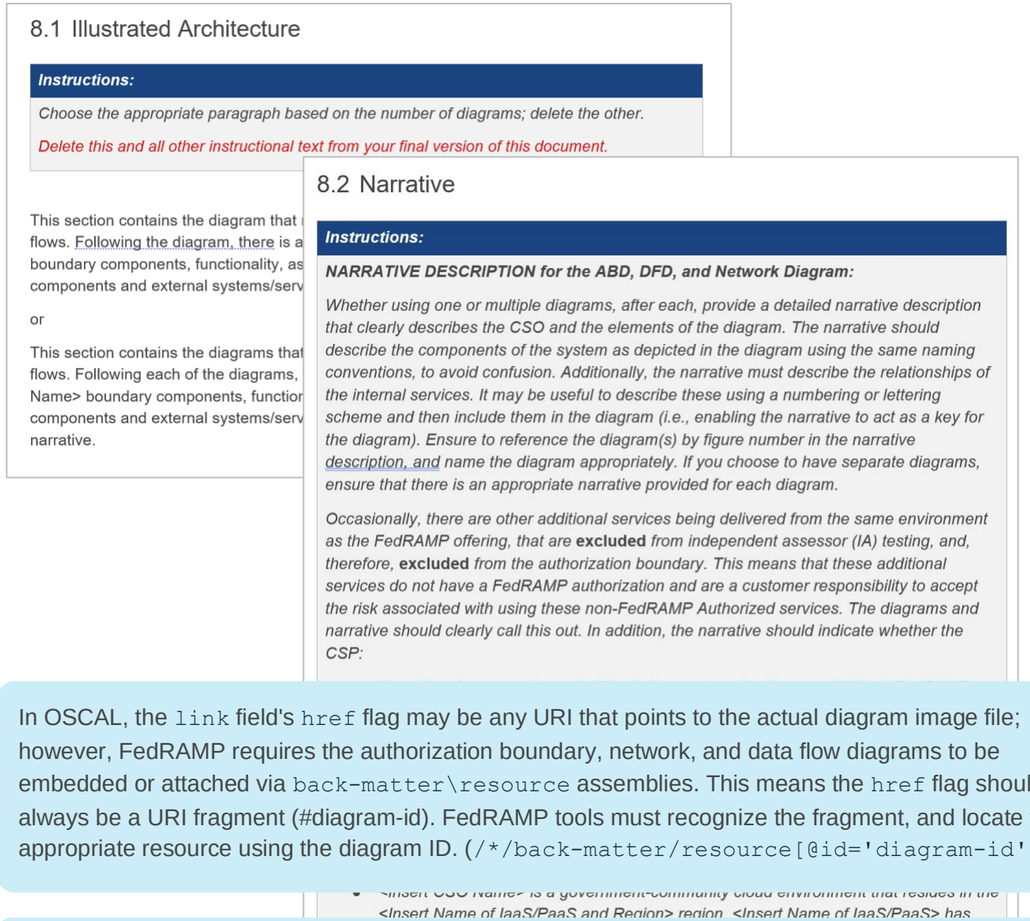
```
<system-characteristics>
    <!-- authorization-boundary -->
    <network-architecture>
        <!-- 8.2 Narrative (Network) -->
        <description>
            <p>A holistic, top-level explanation of the system's network.</p>
        </description>
        <!-- 8.1 Illustrated Architecture (Network) -->
        <diagram uuid="uuid-value">
            <description><p>A diagram-specific explanation.</p></description>
            <link href="#uuid-of-network-diagram-1" rel="diagram" />
            <caption>Network Diagram</caption>
        </diagram>
        <!-- repeat diagram assembly for each additional network diagram -->
    </network-architecture>
    <!-- data-flow -->
</system-characteristics>


<!-- cut -->


<back-matter>
    <!-- citation -->
    <resource uuid=" uuid-of-network-diagram-1">
        <description><p>The primary network architecture diagram.</p></description>
        <rlink href="./diagrams/network.png" media-type="image/png"/>
    </resource>
</back-matter>
```

XPath Queries

```
Overall Description:
  /*/system-characteristics/network-architecture/description/node()

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/network-architecture/diagram)

Link to First Diagram:
  /*/system-characteristics/network-architecture/diagram[1]/link/@href
```

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

```
If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@uuid="uuid-of-network-diagram-1"]/base64
  OR:
  /*/back-matter/resource[@uuid="uuid-of-network-diagram-1"]/rlink/@href

First Diagram Description:
  /*/system-characteristics/network-architecture/diagram[1]/description/node()
```



8.1 Illustrated Architecture

Instructions:

Choose the appropriate paragraph based on the number of diagrams; delete the other.

Delete this and all other instructional text from your final version of this document.

This section contains the diagram that
flows. Following the diagram, there is a
boundary components, functionality, as
components and external systems/serv

or

This section contains the diagrams that
flows. Following each of the diagrams,
Name> boundary components, functior
components and external systems/serv
narrative.

8.2 Narrative

Instructions:

NARRATIVE DESCRIPTION for the ABD, DFD, and Network Diagram:

Whether using one or multiple diagrams, after each, provide a detailed narrative description that clearly describes the CSO and the elements of the diagram. The narrative should describe the components of the system as depicted in the diagram using the same naming conventions, to avoid confusion. Additionally, the narrative must describe the relationships of the internal services. It may be useful to describe these using a numbering or lettering scheme and then include them in the diagram (i.e., enabling the narrative to act as a key for the diagram). Ensure to reference the diagram(s) by figure number in the narrative description, and name the diagram appropriately. If you choose to have separate diagrams, ensure that there is an appropriate narrative provided for each diagram.

Occasionally, there are other additional services being delivered from the same environment as the FedRAMP offering, that are **excluded** *from independent assessor (IA) testing, and, therefore,* **excluded** *from the authorization boundary. This means that these additional services do not have a FedRAMP authorization and are a customer responsibility to accept the risk associated with using these non-FedRAMP Authorized services. The diagrams and narrative should clearly call this out. In addition, the narrative should indicate whether the CSP:*

In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter\resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/back-matter/resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

4.8.3 Data Flow

Representation

```
<system-characteristics>
    <!-- data-flow -->
    <data-flow>
        <!-- 8.2 Narrative (Data Flow) -->
        <description>
            <p>A holistic, top-level explanation of the system's data flows.</p>
        </description>
        <!-- 8.1 Illustrated Architecture (Data Flow) -->
        <diagram uuid="uuid-value">
            <description><p>A diagram-specific explanation.</p></description>
            <link href="#uuid-of-dataflow-diagram-1" rel="diagram" />
            <caption>Data Flow Diagram</caption>
        </diagram>
        <!-- repeat diagram assembly for each additional data flow diagram -->
    </data-flow>
    <!-- network-architecture -->
</system-characteristics>

<!-- cut -->

<back-matter>
    <!-- citation -->
    <resource uuid="uuid-of-dataflow-diagram-1">
        <description><p>The primary data flow diagram.</p></description>
        <base64 filename="data-flow-1.png" media-type="image/png">
            0000<!-- base64 cut -->0000
        </base64>
    </resource>
</back-matter>
```

XPath Queries

```
Overall Description:
  /*/system-characteristics/data-flow/description/node()

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/data-flow/diagram)

Link to First Diagram:
  /*/system-characteristics/data-flow/diagram[1]/link/@href

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

If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@uuid="uuid-of-dataflow-diagram-1"]/base64
  OR:
  /*/back-matter/resource[@uuid="uuid-of-dataflow-diagram-1"]/rlink/@href

First Diagram Description:
  /*/system-characteristics/data-flow/diagram[1]/description/node()
```

Table 9.1 <Insert CSO Name> Services, Ports, and Protocols

Service Name	Port #	Transport Protocol	Reference #	Purpose	Used By

The `description` fields are *Markup multiline* and the `purpose` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

NIST has consolidated OSCAL syntax and is now handling ports, protocols, and services as components. This is a change from the SSP Syntax in Milestone Release 2.

4.9 Ports, Protocols and Services

Entries in the ports, protocols, and services table are represented as `component` assemblies, with the `component-type` flag set to "`service`". Use a `protocol` assembly for each protocol associated with the service. For a single port, set the port-range `start` flag and `end` flag to the same value.

Representation

```
<system-implementation>
    <!-- user -->
    <component uuid="uuid-of-service" type="service">
        <title>[SAMPLE]Service Name</title>
        <description><p>Describe the service</p></description>
        <purpose>Describe the purpose the service is needed.</purpose>
        <link href="uuid-of-component-used-by" rel="used-by" />
        <link href=" uuid-of-component-provided-by" rel="provided-by" />
        <status state="operational" />
        <protocol name="http">
            <port-range start="80" end="80" transport="TCP"/>
        </protocol>
        <protocol name="https">
            <port-range start="443" end="443" transport="TCP"/>
        </protocol>
    </component>
    <!-- Repeat the component assembly for each row in Table 9.1 -->
    <!-- system-inventory -->
</system-implementation>
```

XPath Queries

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

```
Service (1st service):
  /*/system-implementation/component[@type='service'][1]/title

Ports: Start (1st service, 1st protocol, 1st port range):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/port-range[1]/@start

Ports: End (1st service, 1st protocol, 1st port range):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/port-range[1]/@end

Ports: Transport (1st service, 1st protocol, 1st port range):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/port-range[1]/@transport

Protocol (1st service, 1st protocol):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/@name

Purpose (1st service):
  /*/system-implementation/component[@type='service'][1]/purpose

Used By (1st service):
  /*/system-implementation/component[@uuid='uuid-of-component-used-by']/title
```

Appendix Q <CSO Name> Encryption Implementation Status

Data in Transit (DIT)										
	Source				Destination					
Ref #	Areas of DIT[1]	CMVP #[2]	CM Vendr	Module Name	Areas of DIT	CMVP #[3]	CM Vendor	Module Name	Usage	Notes[4]
1	NGINX Server *<Use Case Example - Please Delete>*	#4271 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Red Hat, Inc.	RHEL 8 OpenSSL	All Application Servers	#3980 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Canonical Ltd.	Ubuntu 18.04 OpenSSH Server	Load Balancer TLS to Application Server ☐ TLS 1.1 or earlier ☒ TLS 1.2 ☐ TLS 1.3 ☐ Other _____	
2	All Application Servers *<Use Case Example - Please Delete>*	None ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☐ In FIPS Mode ☐ Other _____	CentOS 7.9	OpenSSL 1.0.1	PostgreSQL	#3980 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Canonical Ltd.	Ubuntu 18.04 OpenSSH Server	Application servers to common DB ☐ TLS 1.1 or earlier ☒ TLS 1.2 ☐ TLS 1.3 ☐ Other _____	Plans to move to RHEL 8. See POA&M ID 111.

[1] Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located.
[2] If using cryptography that lacks FIPS validation, state "No FIPS". If unencrypted, state "Unencrypted".
[3] If using cryptography that lacks FIPS validation, state "No FIPS". If unencrypted, state "Unencrypted".
[4] For example, specify if the historical CM is used or the store lacks encryption entirely. Include the related POA&M ID, remediation plans, etc.

The `link` with `rel="used-by"` is used to identify the component that is using the cryptographic module (e.g., Areas of DIT).

4.10 Cryptographic Modules Implemented for Data-in-Transit (DIT)

NIST's component model treats independent validation of products and services as if that validation were a separate component. This means when using components with FIPS 140 validated cryptographic modules, there must be two `component` assemblies:

- **The Validation Definition**: A component definition that provides details about the validation.
- **The Product Definition**: A component definition that describes the hardware or software product.

The validation definition is a component definition that provides details about the independent validation. Its type must have a value of "validation". In the case of FIPS 140 validation, this must include a `link` field with a `rel` value set to "validation-details". This link must point to the cryptographic module's entry in the NIST Computer Security Resource Center (CSRC) Cryptographic Module Validation Program Database.

The product definition is a product with a cryptographic module. It must contain all of the typical component information suitable for reference by inventory-items and control statements. It must also include a `link` field with a `rel` value set to "validation" and an `href` value containing a URI fragment. The Fragment must start with a hashtag (#) and include the UUID value of the validation component. This links the two together.

Component Representation: Example Product with FIPS 140-2 Validation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->
    <!-- Minimum Required Components -->

    <!-- FIPS 140-2 Validation Certificate Information -->
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="validation">
        <title>Module Name</title>
        <description><p>FIPS 140-2 Validated Module</p></description>
        <prop ns="https://fedramp.gov/ns/oscal" name="asset-type"
              value="cryptographic-module" />
        <prop ns="https://fedramp.gov/ns/oscal" name="vendor-name"
              value="CM Vendor"/>
        <prop ns="https://fedramp.gov/ns/oscal" name="cryptographic-module-usage"
              value="data-at-rest"/>
        <prop name="validation-type" value="fips-140-2"/>
        <prop name="validation-reference" value="0000"/>
        <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" rel="validation-details" />
        <status state="operational" />
    </component>

    <!-- FIPS 140-2 Validated Product -->
    <component uuid="uuid-value" type="software" >
        <title>Product Name</title>
        <description><p>A product with a cryptographic module.</p></description>
        <link href="#uuid-of-validation-component" rel="validation" />
        <status state="operational" />
    </component>

    <!-- service -->
</system-implementation>
<!-- control-implementation -->
```

Data at Rest (DAR)

Ref #	Areas of DAR[5]	CMVP # [6]	CM Vendor Name	Module Name	Usage	Encryption Type	Notes[7]
1	PostgreSQL database *<Use Case Example - Please Delete>*	#3980 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Canonical Ltd.	Ubuntu 18.04 OpenSSL Cryptographic Module	Volume encryption	☒ Full disk ☐ File ☐ Record ☐ None ☐ Other _____	
2	App server local storage *<Use Case Example - Please Delete>*	#2931 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Microsoft	Windows Server 2016	OS and application binaries	☐ Full disk ☒ File ☐ Record ☐ None ☐ Other _____	CM is Historical, per NIST CMVP. Plans to move to Windows 2019 upon Active FIPS-140-validation achieved. See POA&M ID 123.
3	S3 buckets *<Use Case Example - Please Delete>*	#4177 ☒ Embedded CM ☐ Third-party CM ☐ Uses OS CM ☒ In FIPS Mode ☐ Other _____	AWS	Key Management Service (KMS) HSM	Server-side encryption with KMS keys (SSE-KMS) used to encrypt bucket	☒ Full disk ☐ File ☐ Record ☐ None ☐ Other _____	

[5] Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located.
[6] If using cryptography that lacks FIPS validation, state "No FIPS". If unencrypted, state "Unencrypted".
[7] For example, specify if the historical CM is used or the store lacks encryption entirely. Include the related POA&M ID, remediation plans, etc.

The `link` with `rel="used-by"` is used to identify the component that is using the cryptographic module (e.g., Areas of DAR).

4.11 Cryptographic Modules Implemented for Data-at-Rest (DAR)

The approach is the same as in section 4.14 (cryptographic module data-in-transit).

Component Representation: Example Product with FIPS 140-2 Validation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->
    <!-- Minimum Required Components -->

    <!-- FIPS 140-2 Validation Certificate Information -->
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="validation">
        <title>Module Name</title>
        <description><p>FIPS 140-3 Validated Module</p></description>
        <prop ns="https://fedramp.gov/ns/oscal" name="asset-type"
              value="cryptographic-module" />
        <prop ns="https://fedramp.gov/ns/oscal" name="vendor-name"
              value="CM Vendor"/>
        <prop ns="https://fedramp.gov/ns/oscal" name="cryptographic-module-usage"
              value="data-in-transit"/>
        <prop name="validation-type" value="fips-140-3"/>
        <prop name="validation-reference" value="0000"/>
        <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" rel="validation-details" />
        <status state="operational" />
    </component>

    <!-- FIPS 140-2 Validated Product -->
    <component uuid="uuid-value" type="software" >
        <title>Product Name</title>
        <description><p>A product with a cryptographic module.</p></description>
        <link href="#uuid-of-validation-component" rel="validation" />
        <status state="operational" />
    </component>

    <!-- service -->
</system-implementation>
<!-- control-implementation -->
```

Table 12.1 SSP Required Appendices

Appendix Name	Filename
Appendix A: FedRAMP Security Controls (FedRAMP-provided; different template for each impact level)	
Appendix B: Related Acronyms (CSP-provided)	Included within the SSP
Appendix C: Security Policies and Procedures (CSP-provided in a zip file; not required for LI-SaaS)	
Appendix D: User Guide (CSP-provided; not required for LI-SaaS)	
Appendix E: Digital Identity Worksheet (FedRAMP-provided)	Included within the SSP
Appendix F: Rules of Behavior (FedRAMP-provided; not required for LI-SaaS)	
Appendix G: Information System Contingency Plan (ISCP) (FedRAMP-provided; not required for LI-SaaS)	
Appendix H: Configuration Management Plan (CMP) (CSP-provided; not required for LI-SaaS)	
Appendix I: Incident Response Plan (IRP) (CSP-provided; not required for LI-SaaS)	
Appendix J: CIS and CRM Workbook (FedRAMP-provided; different template for each impact level)	
Appendix K: FIPS 199 Worksheet (FedRAMP-provided)	Included within the SSP
Appendix L: CSO-Specific Required Laws and Regulations (CSP-provided)	
Appendix M: Integrated Inventory Workbook (FedRAMP-provided)	
Appendix N: Continuous Monitoring Plan (CSP-provided)	
Appendix O: POA&M (FedRAMP-provided)	
Appendix P: Supply Chain Risk Management Plan (SCRMP) (CSP-provided)	
Appendix Q: Cryptographic Module Table (FedRAMP-provided)	

5 Attachments

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The resource's `title` and `description` must be used to provide a human-readable indicator of what attachment is being referenced, however, OSCAL extensions must also be provided when applicable for machine readability. The following table describes how each attachment is handled:

Appendix Name	Machine Readable	How to Handle in OSCAL
Appendix A: FedRAMP Security Controls	Yes	This can be generated from the content in the Security Controls section and does not need to be maintained separately or attached.
Appendix B: Related Acronyms	No	Attach using the back-matter, resource syntax. For Acronyms, resource must include a prop with @ns="https://fedramp.gov/ns/oscal", @name="type", and @value="fedramp-acronyms".
Appendix C: Security Policies and Procedures	No	Attach using the back-matter, resource syntax. For Policies, resource must include a prop with @name="type", @value="policy", and @class="control-family". For Procedures, resource must include a prop with @name="type", @value="procedure", and @class="control-family".
Appendix D: User Guide	No	Attach using the back-matter, resource syntax. For User Guides, resource must include a prop with @name="type" and @value="users-guide".
Appendix E: Digital Identity Worksheet	Yes	Incorporated above. See the Digital Identity Determination Section.
Appendix F: Rules of Behavior	No	Attach using the back-matter, resource syntax. For Rules of Behavior, resource must include a prop with @name="type" and @value="rules-of-behavior".
Appendix G: Information System Contingency Plan (ISCP)	No	Attach using the back-matter, resource syntax. For ISCP, resource must include a prop with @name="type", @value="plan", and @class="information-system-contingency-plan".
Appendix H: Configuration Management Plan (CMP)	No	Attach using the back-matter, resource syntax. For CMP, resource must include a prop with @name="type", @value="plan", and @class="configuration-management-plan".
Appendix I: Incident Response Plan (IRP)	No	Attach using the back-matter, resource syntax. For IRP, resource must include a prop with @name="type", @value="plan", and @class="incident-response-plan".
Appendix J: CIS and CRM Workbook	Yes	This can be generated from the content in the Security Controls section and does not need to be maintained separately or attached.
Appendix K: FIPS 199 Worksheet	Yes	Incorporated above. See the Security Objectives Categorization (FIPS-199) Section.
Appendix L: CSO-Specific Required Laws and Regulations	No	Attach using the back-matter, resource syntax. For User Guides, resource must include a prop with @name="type" and @value="law".

Appendix Name	Machine Readable	How to Handle in OSCAL
Appendix M: Integrated Inventory Workbook	Yes	See the System Inventory Section.
Appendix N: Continuous Monitoring Plan	No	Attach using the back-matter, resource syntax. For ConMon, resource must include a prop with @name="type", @value="plan", and @class="incident-response-plan".
Appendix O: POA&M	Yes	This is maintained separately in an OSCAL POA&M but can be attached using the back-matter, resource syntax. For POA&M, resource must include a prop with @name="type", @value="plan", and @class="poam".
Appendix P: Supply Chain Risk Management Plan (SCRMP)	No	Attach using the back-matter, resource syntax. For SCRMP, resource must include a prop with @name="type", @value="plan", and @class="scrmp".
Appendix Q: Cryptographic Module Table	Yes	See the Cryptographic Modules Section dealing with components.

Table 12.1 SSP Required Appendices

Appendix Name	Filename
Appendix A: FedRAMP Security Controls (FedRAMP-provided; different template for each impact level)	
Appendix B: Related Acronyms (CSP-provided)	Included within the SSP
Appendix C: Security Policies and Procedures (CSP-provided in a zip file; not required for LI-SaaS)	
Appendix D: User Guide (CSP-provided; not required for LI-SaaS)	
Appendix E: Digital Identity Worksheet (FedRAMP-provided)	Included within the SSP
Appendix F: Rules of Behavior (FedRAMP-provided; not required for LI-SaaS)	
Appendix G: Information System Contingency Plan (ISCP) (FedRAMP-provided; not required for LI-SaaS)	
Appendix H: Configuration Management Plan (CMP) (CSP-provided; not required for LI-SaaS)	
Appendix I: Incident Response Plan (IRP) (CSP-provided; not required for LI-SaaS)	
Appendix J: CIS and CRM Workbook (FedRAMP-provided; different template for each impact level)	
Appendix K: FIPS 199 Worksheet (FedRAMP-provided)	Included within the SSP
Appendix L: CSO-Specific Required Laws and Regulations (CSP-provided)	
Appendix M: Integrated Inventory Workbook (FedRAMP-provided)	
Appendix N: Continuous Monitoring Plan (CSP-provided)	
Appendix O: POA&M (FedRAMP-provided)	
Appendix P: Supply Chain Risk Management Plan (SCRMP) (CSP-provided)	
Appendix Q: Cryptographic Module Table (FedRAMP-provided)	

5.7 Attachments

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The following table describes how each attachment is handled:

Attachment Representation

```
<!-- cut -->
<back-matter>
    <resource uuid="uuid-value">
        <title>Document Title</title>
        <desc>Policy document</desc>
        <prop name="type" ns="https://fedramp.gov/ns/oscal" value="policy"/>
        <prop name="publication" ns="https://fedramp.gov/ns/oscal" value="2021-01-01Z"/>
        <prop name="version" ns="https://fedramp.gov/ns/oscal" value="1.2"/>
        <!-- Add rlink with relative path or embed with base64 encoding -->
        <base64>00000000</base64>
    </resource>
    <resource uuid="uuid-value" />
    <!-- cut: policies 3 - 13 -->
    <resource uuid="uuid-value" />
    <resource uuid="uuid-value" />
    <!-- cut: procedure 2 - 13 -->
</back-matter>
```

FedRAMP Extensions & Accepted Values

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

- `name="type"`
- `name="title"`
- `name="publication"`
- `name="version"`

XPath Queries

```
The Number of Policies Attached:
  count(/*/back-matter/resource/prop[@name="type"]
  [@ns="https://fedramp.gov/ns/oscal"][string(./@value)="policy"])

Attachment (Embedded Base64 encoded):
  /*/back-matter/resource[@id="att-policy-1"]/base64
  OR (Relative Link):
  /*/back-matter/resource[@id="att-policy-1"]/rlink/@href

Title of First Policy Document:
  /*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
  [string(.)="policy"][1]/../prop[@name="title"][@ns="https://fedramp.gov/ns/oscal"]
```

Replace "policy" with "plan", "rob", etc. for each attachment type.

Appendix M <Insert CSO Name> Integrated Inventory Workbook (IIW)

Instructions:

This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).

Security control CM-8 requires CSPs to develop and document an inventory of system components within the authorization boundary that is at the level of granularity deemed necessary for tracking and reporting. To this end, FedRAMP provides an Integrated Inventory Workbook (IIW) Template that CSPs must complete and submit as Appendix M of the SSP. Instructions for completing the IIW are provided in the template.

Consistency is key to providing a good SSP. The inventory should be consistent with what is depicted in the SSP diagrams. SSP reviewers should not have any issues identifying the key inventory components, as these are represented in the SSP diagram.

*CSPs are also required to update the IIW as part of **monthly** continuous monitoring efforts.*

Delete this and all other instructional text from your final version of this document.

The <Insert CSO Name> integrated inventory workbook is included in Appendix M, attached separately.

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No

Software and Database Inventories				Any Inventory				
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner
Acme Software	Acme CloudApp v1.0		CRM					

NOTE: OSCAL also uses components to represent content that does not typically appear in the system inventory. When rendering a presentation of system inventory, tools should offer users the option to exclude components such as:

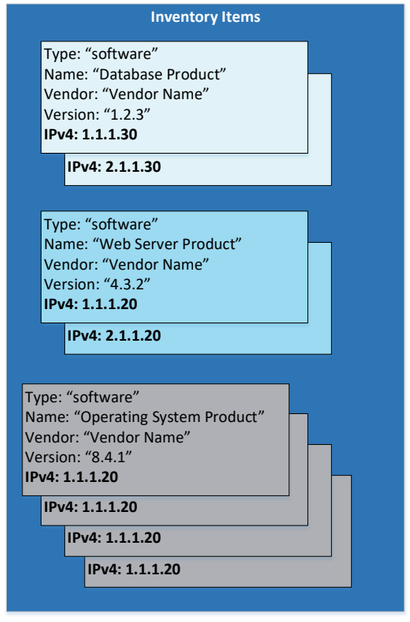
Interconnections, services, policies, procedures, the system (as a whole), leveraged systems (as a whole), and FIPS 140 validation details.

5.8 System Inventory Approach

OSCAL makes two approaches available for depicting the system inventory:

- **Flat-File Approach**: Similar to today's FedRAMP Integrated inventory workbook where all of the information on a spreadsheet row is captured in a single assembly.
- **Component-Based Approach**: A component is defined once with as much known detail as possible, and inventory-items point to components for common information.

FedRAMP prefers the component-based approach but accepts the flat-file approach to aid CSPs who are converting their existing MS-Excel based FedRAMP Integrated Inventory Workbook to OSCAL. **FedRAMP SSP tools must support both approaches.**

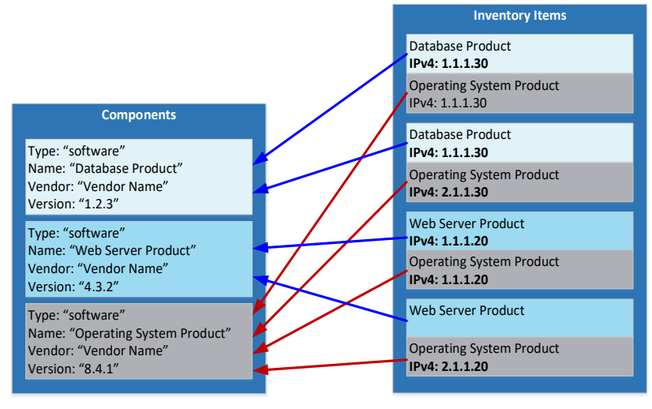


Flat-File Inventory Approach

With the **flat-file approach**, all content on a spreadsheet row appears in a single OSCAL `inventory-item` assembly. This results in a great deal of redundant information but is a simple transition from the current spreadsheet approach.

With the **component-based approach**, common information is captured once in a `component` assembly. Each instance of that component has its own `inventory-item` assembly, which cites the relevant component and only includes information unique to that instance.

For example, if the same Linux operating system is used as the platform for all database and web servers, most of the details about the Linux operating system can be captured once as a `component`. This includes information such as vendor name, version number, and patch level. If four Linux instances are used, each instance is an `inventory item` with a unique IP address and MAC address. Only those unique pieces are captured at the inventory level. All four inventory-items point back to the `component` for vendor name, version number, and patch level.



Component-based Inventory Approach

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No		
Software Example	123.45.78.400	123.45.78.400	No		
Database Example	123.45.78.401	123.45.78.401	No		

FedRAMP Extensions & Allowed Values

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

- name="vendor-name"
- name="scan-type"
  - **Valid:** infrastructure, web, database, container

OS/Infrastructure Inventory							
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Mo
linux01	00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Ser

NIST Allowed Values

prop

- name="virtual"
  - **Valid:** yes, no
- name="public"
  - **Valid:** yes, no

prop

- name="allows-authenticated-scan"
  - **Valid:** yes, no
- name="is-scanned"
  - **Valid:** yes, no

Software and Database Inventories				Ang Inventory			
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner
Acme Software	Acme CloudApp v1.0		CRM				
Oracle	Oracle v11		Records Management				

FedRAMP Allowed Values

prop

- name="asset-type"
  - **Valid:** operating-system, database, web-server, dns-server, email-server, directory-server, pbx, firewall, router, switch, storage-array

Other values are allowed for now.

Software and Database Inventories				
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

5.8.1 Flat File Approach

Flat-File Representation

```
<!-- cut -->
<system-implementation>
    <!-- interconnection -->
    <system-inventory>
        <inventory-item uuid="uuid-value" asset-id="unique-asset-id">
            <description><p>Flat-File Example (No implemented-c
            <prop name="ipv4-address" value="0.0.0.0"/>
            <prop name="ipv6-address" value="0000:0000:0000:000
            <prop name="virtual" value="no"/>
            <prop name="public" value="no"/>
            <prop name="fqdn" value="example.com"/>
            <prop name="uri" value="https://example/query?key=v
            <prop name="netbios-name" value="netbios-name"/>
            <prop name="mac-address" value="00:00:00:00:00:00"/
            <prop name="software-name" value="software-name"/>
            <prop name="version" value="V 0.0.0"/>
            <prop name="asset-type" value="os"/>
            <prop name="vendor-name" value="Vendor Name"/>
            <prop name="model" value="Model Number"/>
            <prop name="patch-level" value="Patch-Level"/>
            <prop name="serial-number" value="Serial #"/>
            <prop name="asset-tag" value="Asset Tag"/>
            <prop name="vlan-id" value="VLAN Identifier"/>
            <prop name="network-id" value="Network Identifier"/
            <prop name="scan-type" ns="https://fedramp.gov/ns/o
            <prop name="allows-authenticated-scan"  value="no">
                <remarks><p>If no, explain why. If yes, omit re
            </prop>
            <prop name="baseline-configuration-name" value="Baseline Config. Name" />
            <prop name="physical-location" value="Physical location of Asset" />
            <prop name="is-scanned" value="yes"/>
            <prop name="function" value="Required brief, text-based description."/>
            <link rel="validation" href="#uuid-of-validation-component" />
            <status state="operational"/>
            <responsible-party role-id="asset-owner">
                <party-id>person-7</party-id>
            </responsible-party>
            <responsible-party role-id="asset-administrator">
                <party-id>it-dept</party-id>
            </responsible-party>
            <implemented-component component-uuid="component-uuid-value " />
            <remarks><p>COMMENTS: Additional information about this item.</p></remarks>
        </inventory-item>
        <!-- Repeat the inventory-item assembly for each item in the inventory -->
    </system-inventory>
    <!-- system-implementation remarks -->
</system-implementation>
```

NIST-Defined Identifier

Required Role ID may be one of the following:

- asset-owner
- asset-administrator
- security-operations
- network-operations
- incident-response
- helpdesk
- configuration-management
- maintainer
- provider

Other values are allowed.

XPath Queries

See Section 5.8.3, Inventory Data Locations and XPath Queries

NOTES:

The value of `asset-type` determines whether the identified asset-administrator is managing a system or an application. Currently, any FedRAMP-defined `asset-type` implies the management of a system, and therefore, is to be scanned as infrastructure.

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No		
Software Example	123.45.78.400	123.45.78.400	No		
Database Example	123.45.78.401	123.45.78.401	No		

FedRAMP Extensions & Allowed Values

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

- name=""vendor-name""
- name="scan-type"
  - **Valid:** infrastructure, web, database, container

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00:00	Yes	Base Config1	CentOS 5.1				

FedRAMP Allowed Values

prop

- name="asset-type"
  - **Valid:** os, database, web-server, dns-server, email-server, directory-server, pbx, firewall, router, switch, storage-array

Other values are allowed for now.

Software and Database Inventories							
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

5.8.2 Component-based Approach

Component-based Representation

```
<!-- cut -->
<system-implementation>
    <component uuid="uuid-value" type="software">
        <prop name="virtual" value="no"/>
        <prop name="software-name" value="software-name"/>
        <prop name="version" value="V 0.0.0"/>
        <prop name="asset-type" value="operating-system"/>
        <prop name="vendor-name" value="Vendor Name"/>
        <prop name="model" value="Model Number"/>
        <prop name="patch-level" value="Patch-Level"/>
        <prop name="scan-type" ns="https://fedramp.gov/ns/oscal" value="infrastructure"/>
        <prop name="allows-authenticated-scan"  value="no">
            <remarks><p>If no, explain why. If yes, omit remarks field.</p></remarks>
        </prop>
        <prop name="baseline-configuration-name" value="Baseline Config. Name" />
        <prop name="function" value="Required brief, text-based description.">
            <remarks><p>Optional, longer, formatted description.</p></remarks>
        </prop>
        <link rel="validation" href="#uuid-of-validation-component" />
        <status state="operational"/>
        <responsible-party role-id="asset-owner">
            <party-id>person-7</party-id>
        </responsible-party>
        <responsible-party role-id="asset-administrator">
            <party-id>it-dept</party-id>
        </responsible-party>
    </component>
    <!-- service, interconnection -->
    <system-inventory>
        <inventory-item uuid="uuid-value" asset-id="unique-asse
            <description><p>If needed, describe this instance.<
            <prop name="ipv4-address" value="0.0.0.0"/>
            <prop name="public" value="no"/>
            <prop name="fqdn" value="example.com"/>
            <prop name="uri" value="https://example/query?key=v
            <prop name="mac-address" value=">00:00:00:00:00:00"
            <prop name="serial-number" value="Serial #"/>
            <prop name="vlan-id" value="VLAN Identifier"/>
            <prop name="network-id" value="Network Identifier"/
            <prop name="is-scanned" value="yes" />
            <implemented-component component-uuid="component-uu
            <remarks><p>COMMENTS: Additional information about
        </inventory-item>
        <!-- Repeat the inventory-item assembly for each use of
    </system-inventory>
    <!-- system-implementation remarks -->
</system-implementation>
```

NIST-Defined Identifier

Required Role ID may be one of the following:

- asset-owner
- asset-administrator
- security-operations
- network-operations
- incident-response
- helpdesk
- configuration-management
- maintainer
- provider

Other values are allowed.

XPath Queries

See Section 5.8.3, Inventory Data Locations and XPath Queries

NOTES:

- If component-sample is an image of a Linux virtual machine (VM), and 10 instances of that VM are in use, there would be one (1) component assembly and ten (10) inventory-item assemblies, all referencing the same component.

5.8.3 Inventory Data Locations and XPath Queries

The following queries are intended to show where to find each piece of information within the system inventory template.

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES

All Inventories	**UNIQUE ASSET IDENTIFIER**	Unique Identifier associated with the asset. This Identifier should be used consistently across all documents, 3PAOs artifacts, and any vulnerability scanning tools. For OS/Infrastructure and Web Application Software, this is typically an IP address or URL/DNS name. For a database, it is typically an IP address, URL, or database name. A CSP's own naming scheme is also acceptable as long as it has unique identifiers.	Must be unique.	Mandatory for all inventory records.		X	1	`/*/system-implementation/system-inventory/inventory-item/prop[@asset-id="___"]/@value`
								OR
								`/*/system-implementation/component/prop[@name="asset-id"]/@value`
									The system-specific "Unique Asset Identifier" must be set as the asset-id flag on the inventory-item field.

	IPv4 or IPv6 Address	If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column.
		
		If a device has multiple IP addresses, then include one row in this inventory for each IP address.
				Optional, unless used as Identifier in vulnerability scans or security assessments.		X	0 - ∞	`/*/system-implementation/system-inventory/inventory-item/prop[@name="ipv4-address"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="ipv6-address"]/@value`
									One prop field per IP address, if more than one.

	Virtual	Is this asset virtual?	Yes or No.	Mandatory for OS/Infrastructure. Software, and Database.	X	X	1	`/*/system-implementation/component/prop[@name="virtual"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="virtual"]/@value`
									Must have "Virtual" at the inventory item-level either explicitly, or via a linked component.
									
									May define it at component level and propagate to inventory-item.

	Public	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	Yes or No.	Mandatory for OS/Infrastructure. Software, and Database.		X	1	`/*/system-implementation/system-inventory/inventory-item/prop[@name="public"]/@value`	

	DNS Name or URL	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	Valid DNS name or URL.	Optional, unless used as Identifier in vulnerability scans or security assessments.		X	0 - ∞	`/*/system-implementation/system-inventory/inventory-item/prop[@name="fqdn"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="uri"]/@value`
									May use either DNS name, URL, or both. Use a separate prop field for each DNS name and/or URL.

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
OS/Infrastructure Inventory	**NetBIOS Name**	If available, state the NetBIOS name. May be left blank if one does not exist, or dynamic.	Valid NetBIOS name.	Optional, unless used as Identifier in scans or security assessments.		X	0 - ∞	`/*/system-implementation/system-inventory/inventory-item/prop[@name="netbios-name"]/@value`	One prop field per NetBIOS name, if more than one.
	MAC Address	If available, state the MAC Address. May be left blank if one does not exist, or dynamic.	Valid MAC Address.	Optional, unless used as Identifier in scans or security assessments.		X	0 - ∞	`/*/system-implementation/system-inventory/inventory-item/prop[@name="mac-address"]/@value`	One prop field per MAC address, if more than one.
	Authenticated Scan	Is the asset is planned for an authenticated scan?	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	1	`/*/system-implementation/component/prop[@name="allows-authenticated-scan"]/@value` `/*/system-implementation/system-inventory/inventory-item/prop[@name="allows-authenticated-scan"]/@value`	Must have “Authenticated-Scan” at the inventory-item level either explicitly or via a linked component. May define it at component level and propagate to inventory-item.
	Baseline Configuration Name	If available, provide the name of the configuration template used within the CSP configuration management.	.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	0 or 1	`/*/system-implementation/component/prop[@name="baseline-configuration-name"]/@value` `/*/system-implementation/system-inventory/inventory-item/prop[@name="baseline-configuration-name"]/@value`	Must have “Baseline Configuration Name” at the inventory-item level either explicitly or via a linked component. May define it at component level and propagate to inventory-item.

	OS Name and Version	Operating System Name and Version running on the asset.		Optional for OS/Infrastructure. Leave blank for Software and Database.		X	0 or 1	`/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								`/*/system-implementation/component/prop[@name="version"]/@value`
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]/@value`
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]/@value`
									Use software name and version and set asset-type of “os”.
									Required for operating systems.
									Must have “OS Name and Version” at the inventory-item level either explicitly or via a linked component. May define it at the component level and propagate to inventory item.

	Location	Physical location of hardware. Could include Data Center ID, Cage#, Rack# or other meaningful location identifiers.	Valid locations for CSP infrastructure.	Optional for OS/Infrastructure. Leave blank for Software and Database.		X	0 or 1	`/*/system-implementation/system-inventory/inventory-item/prop[@name="physical-location"]/@value`	
	Asset Type	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.)		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	1	`/*/system-implementation/component/prop[@name="asset-type"]/@value` `/*/system-implementation/system-inventory/inventory-item[@name="asset-type"]/@value`	Must use an Accepted Value (see Registry) if an applicable one exists. Must have “Asset Type” at the inventory-item level, either explicitly or via a linked component. May define it at component level and propagate to inventory-item.

	Hardware Make/Model	Name of the hardware product and model.		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	0 or 1	`/*/system-implementation/component/prop[@name="vendor-name"]/@value`
								`/*/system-implementation/component/prop[@name="model"]/@value`
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="hardware-model"]/@value`
									Must have “Hardware Vendor” and “Hardware Model” at the inventory item-level either explicitly, or via a linked component. May define it at component level and propagate to inventory-item.
									NOTE: @name=“model” at component level, but @name=“hardware-model” at inventory level.

	In Latest Scan	Should the asset appear in the network scans, and can it be probed by the scans creating the current POA&M?	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.		X	1	`/*/system-implementation/system-inventory/inventory-item/prop[@name="is-scanned"]/@value`	

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES

Software and Database Inventories	**Software/ Database Vendor**	Name of Software or Database vendor.	If open source (e.g., there is no "vendor), enter "Open Source" as the vendor name.	Mandatory for Software and Database. Leave blank for OS/Infrastructure.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
									Must have "Software/Database Vendor" at the inventory-item level either explicitly or via a linked component.
									
									May define it at component level and propagate to inventory-item.

	Software/ Database Name & Version	Name of Software or Database product and version number.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								
								`/*/system-implementation/component/prop[@name="version"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]/@value`
									Required for software or database. Omit for OS/Infrastructure

	Patch Level	If applicable.		Optional if applicable. Otherwise, leave blank.	**X**	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="patch-level"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-patch-level"]/@value`
									The "Patch Level" may be specified at the component or inventory-item level.

	Function	For Software or Database, the function provided by the Software or Database for the system.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="function"]/@value`
								
								`/*/system-implementation/component/prop[@name="function"]/remarks`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="function"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="function"]/remarks`
									Must have a brief, text-base "function" description in the value flag at the inventory item-level.
									
									May define it at component level and propagate to inventory-item.
									
									May have a separate "function" at the component level.
									
									May have an expanded, formatted function description in the remarks.

.

		Guidance	Valid Values	Requirement	Component	Inventory -Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
Any Inventory	**Comments**	Any additional information that could be useful to the reviewer.		Optional for OS/Infrastructure, Software and Database.	X	X	**0 or 1**	/*/system-implementation/component/remarks /*/system-implementation/system-inventory/inventory-item/remarks	May have comments in either the component level, inventory-item level, or both.
	Serial #/Asset Tag#	Product serial number or internal asset tag #.		Optional for OS/Infrastructure, Software, and Database.		**X**	**0 or 1**	/*/system-implementation/system-inventory/inventory-item/prop[@name="serial-number"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="asset-tag"]/@value	
	VLAN/ Network ID	Virtual LAN or Network ID.		Optional for OS/Infrastructure, Software, and Database.		**X**	**0 - ∞**	/*/system-implementation/system-inventory/inventory-item/prop[@name="vlan-id"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="network-id"]/@value	
	System Administrator/ Owner	Name of the system administrator or owner.		Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	X	**X**	**0 - ∞**	COMPONENT OWNER (Person): /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-uuid]/name COMPONENT ADMINISTRATOR (Org): /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-uuid]/name INVENTORY ITEM OWNER (Person): /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-uuid]/name INVENTORY ITEM ADMINISTRATOR (Org): /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-uuid]/name	Must have “System Owner/Administrator” at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate “system owner/administrator” at the component level.
	Application Administrator/ Owner	Name of the application administrator or owner.		Optional for OS/Infrastructure, Software, and Database.	X	**X**	**0 - ∞**	COMPONENT OWNER: /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-uuid]/name CMPONENT ADMINISTRATOR: /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-uuid]/name INVENTORY ITEM OWNER: /*/metadata/party[@id=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-id]/person/person-name INVENTORY ITEM ADMINISTRATOR: /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-uuid]/name	Must have “Application Owner/Administrator” at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate “system owner/administrator” at the component level.
ADDITIONAL	**Scan Type**	Indicate which scan type(s) the item is subjected to.	infrastructure, database, web	Mandatory	X	**X**	**1 - ∞**	/*/system-implementation/component/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]/@value	Valid values: infrastructure, web, database. If more than one type is applicable, use one field per type.
	FIPS 140-2 Validation	Indicate the certificate information for an inventory item with a FIPS 140-2 validated cryptographic module.	component-id	Mandatory for any item involving cryptography. Omit otherwise.	X	**X**	**1w - ∞**	/*/system-implementation/component/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]/@value	If an item has more than one cryptographic module, use one entry per validation certificate. May define “FIPS 140-2 validation” at the component level and propagate to the inventory-item level.

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No

Software and Database Inventories				Any Inventory				
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner
Acme Software	Acme CloudApp v1.0		CRM					
Oracle	Oracle v11		Records Management					

XPath Queries

```
Number of Inventory Items:
  count(/*/system-implementation/system-inventory/inventory-item)

Number of Hardware Components:
  count(/*/system-implementation/component[@type="hardware"])

Number of Software Components:
  count(/*/system-implementation/component[@type="software"])

In Latest Scan?:
  /*/system-implementation/system-inventory/inventory-item[1]/prop[@name="is-
  scanned"]/@value

List Inventory Items Not Scanned:
  /*/system-implementation/system-inventory/inventory-item/prop[@name="is-
  scanned"][@value='no']/../prop[@name='ipv4-address']

List of Reasons Inventory Items Were Not Scanned:
  /*/system-implementation/system-inventory/inventory-item/prop[@name="is-
  scanned"][@value='no']/remarks/node()
```

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

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/reference/datatypes/

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

All Inventories			
IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column. If a device has multiple IP addresses, then include one row in this inventory for each IP address.	Is this asset virtual?	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.
	Yes or No.	Yes or No.	Valid DNS name or URL.
Optional, unless used as Identifier in vulnerability scans or security assessments.	Mandatory for OS/Infrastructure, Software, and Database.	Mandatory for OS/Infrastructure, Software, and Database.	Optional, unless used as Identifier in vulnerability scans or security assessments.

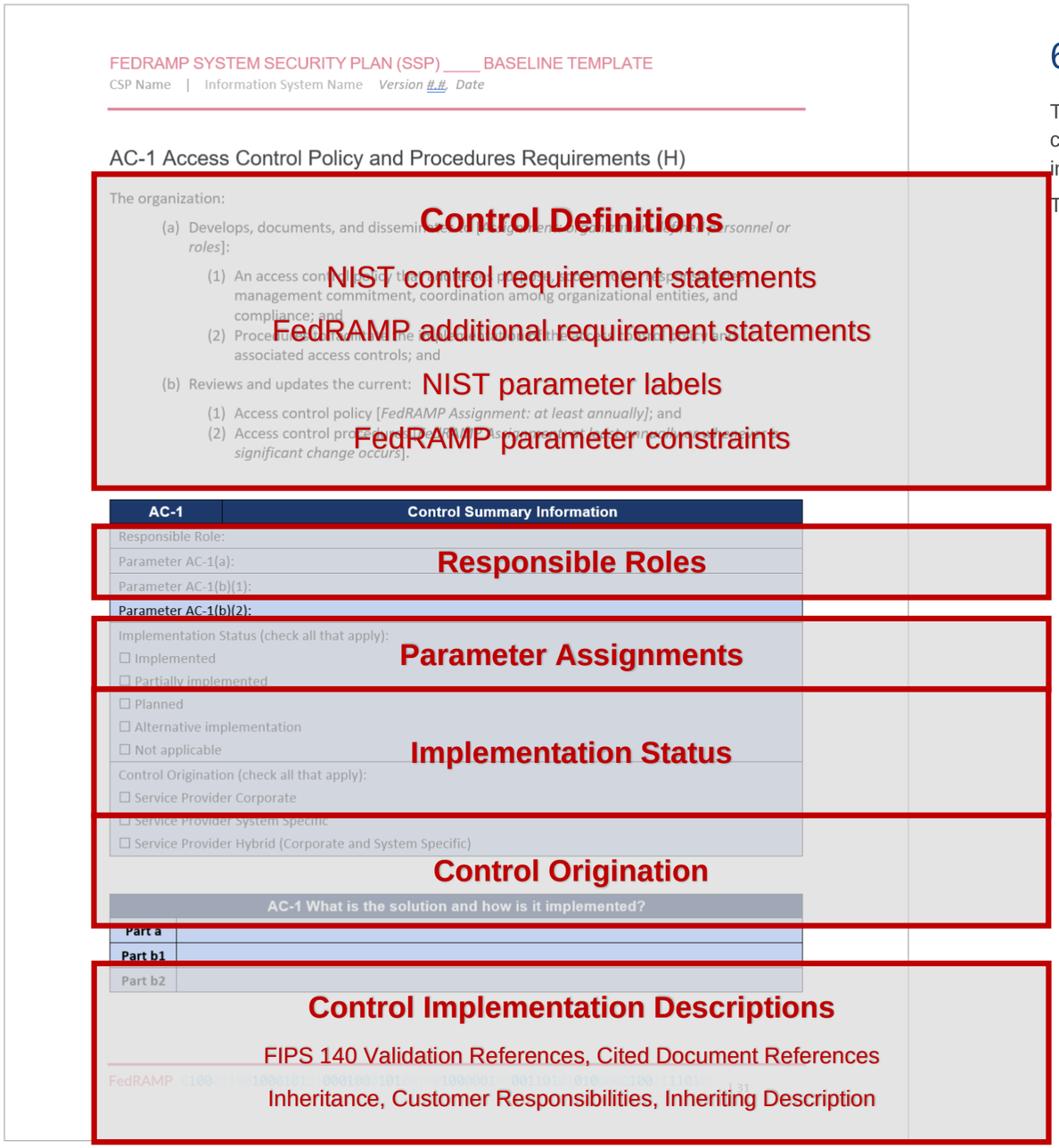
Any Inventory				
Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner
Any additional information that could be useful to the reviewer.	Product serial number or internal asset tag #.	Virtual LAN or Network ID.	Name of the system administrator or owner.	Name of the application administrator or owner.
Optional for OS/Infrastructure, Software and Database.	Optional for OS/Infrastructure, Software, and Database.	Optional for OS/Infrastructure, Software, and Database.	Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	Optional for OS/Infrastructure, Software, and Database.

Unlike most XPath 2.0 queries in this document, the following queries cannot be easily converted to XPath 1.0. If working with XPath 1.0, it may be necessary to perform each search with two separate queries. These queries will list all the IPv4 addresses for each scan type (infrastructure, web, and database), whether using the flat-file inventory approach or the component-based approach.

XPath 2.0 Queries

```
IPv4 Address of All Inventory Items Identified for Infrastructure Scanning:
  distinct-values( (let $key:=/*/system-implementation/component[prop [@name='scan-type']
  [@ns='https://fedramp.gov/ns/oscal']='infrastructure']/@uuid return /*/system-
  implementation/system-inventory/inventory-item [implemented-component/@component-
  uuid=$key]/ prop[@name='ipv4-address']) | (/*/system-implementation/system-
  inventory/inventory-item/prop[@name='ipv4-address'][../prop[@name='scan-
  type'][@ns='https://fedramp.gov/ns/oscal']  [string(.)='infrastructure']]) )

IPv4 Address of All Inventory Items Identified for Web Scanning:
  distinct-values( (let $key:=/*/system-implementation/component[prop[@name='scan-type']
  [@ns='https://fedramp.gov/ns/oscal']='web']/@uuid return /*/system-implementation/system-
  inventory/inventory-item [implemented-component/@component-uuid=$key]/prop[@name='ipv4-
  address']) | (/*/system-implementation/system-inventory/inventory-item/prop[@name='ipv4-
  address'][../prop[@name='scan-type'][@ns='https://fedramp.gov/ns/oscal'][string(.)='web']]))

IPv4 Address of All Inventory Items Identified for Database Scanning:
  distinct-values( (let $key:=/*/system-implementation/component[prop [@name='scan-type']
  [@ns='https://fedramp.gov/ns/oscal']='database']/@uuid return /*/system-implementation/
  system-inventory/inventory-item [implemented-component/@component-uuid=$key]/
  prop[@name='ipv4-address']) | (/*/system-implementation/system-inventory/inventory-item/
  prop[@name='ipv4-address'][../prop[@name='scan-type'][@ns='https://fedramp.gov/ns/oscal']
  [string(.)='database']]))

IPv4 Address of All Items Where an Authenticated Scan is Possible:
  distinct-values( (/*/system-implementation/system-inventory/inventory-item/prop
  [@name='ipv4-address'][../prop[@name="allows-authenticated-scan"][@value='yes']] ) | (let
  $key:=/*/system-implementation/component[prop [@name='allows-authenticated-
  scan'][@value='yes']]/@uuid return /*/system-implementation/system-inventory/inventory-item
  [implemented-component/@component-uuid=$key]/prop[@name='ipv4-address']))

IPv4 Address of All Items Where an Authenticated Scan is Not Possible:
  distinct-values( (/*/system-implementation/system-inventory/inventory-item/
  prop[@name='ipv4-address'][../prop[@name="allows-authenticated-scan"][@value='no']] ) | (
  let $key:=/*/system-implementation/component[prop [@name='allows-authenticated-
  scan'][@value='no']]/@uuid return /*/system-implementation/system-inventory/inventory-item
  [implemented-component/@component-uuid=$key]/prop[@name='ipv4-address']) )

Authenticated Scan Justification (if Authenticate Scan is "no"):
  /*/system-implementation/system-inventory/inventory-item/prop[@name="allows-
  authenticated-scan"][@value="no"]/remarks/node()

OR
  /*/system-implementation/component/prop[@name="allows-authenticated-scan"]
  [@value="no"]/remarks/node()
```

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/reference/datatypes/



6 Security Controls

This section describes the modeling of security control information in an OSCAL-based FedRAMP SSP. To ensure consistent processing, FedRAMP imposes specific requirements on the use of OSCAL for control implementation information.

The modeling of controls is addressed in the following sections as follows:

- **Section 6.1, Control Definitions**
- **Section 6.2, Responsible Roles Responsible Roles** and Parameter Assignments
- **Section 6.3, Implementation Status**
- **Section 6.3.1.1, Control Origination**
- **Section 6.4, Control Implementation Descriptions**
    - **Organization**
        - **Policy and Procedure Statements**
        - **Multi-Part Statements**
        - **Single Statements**
    - **Response**
        - **Overview**
        - **Example**
        - **“This System”**
        - **Inheriting from a Leveraged Authorization**
        - **Identifying Customer Responsibilities**
        - **Providing Inheritance**

This section provides the preferred approach to representing controls in OSCAL. For system owners converting their MS Word-based SSP to OSCAL, see *7.4, Converting a Legacy SSP to OSCAL* for an alternative OSCAL control representation, which aligns better with legacy SSP content.

AC-2 Account Management (L) (M) (H)

The organization:

(a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

(a) Assigns account managers for information system accounts;

(b) Establishes conditions for group and role membership;

(c) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

(d) Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;

(e) Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

(f) Monitors the use of information system accounts;

(g) Notifies account managers:

(1) When accounts are no longer required;
(2) When users are terminated or transferred; and
(3) When individual information system usage or need-to-know changes;

(h) Authorizes access to the information system based on:

(1) A valid access authorization;
(2) Intended system usage; and
(3) Other attributes as required by the organization or associated missions/business functions;

(i) Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: monthly for privileged accessed, every six (6) months for non-privileged access*]; and

(j) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	

6.1 Control Definitions

All control definition information is imported from the appropriate FedRAMP baseline (OSCAL profile). This includes the original NIST control definition and parameter labels as well as any FedRAMP control guidance and parameter constraints.

Interpreting and presenting profile content is beyond the scope of this document. Please refer to the NIST OSCAL Profile and Catalog schema references for more information:

- Profile Model
- Catalog Reference

Only the control implementation information is present within an OSCAL-based SSP. Each control in the FedRAMP baseline must have a corresponding `implemented-requirement` assembly in the `control-implementation` assembly.

Representation

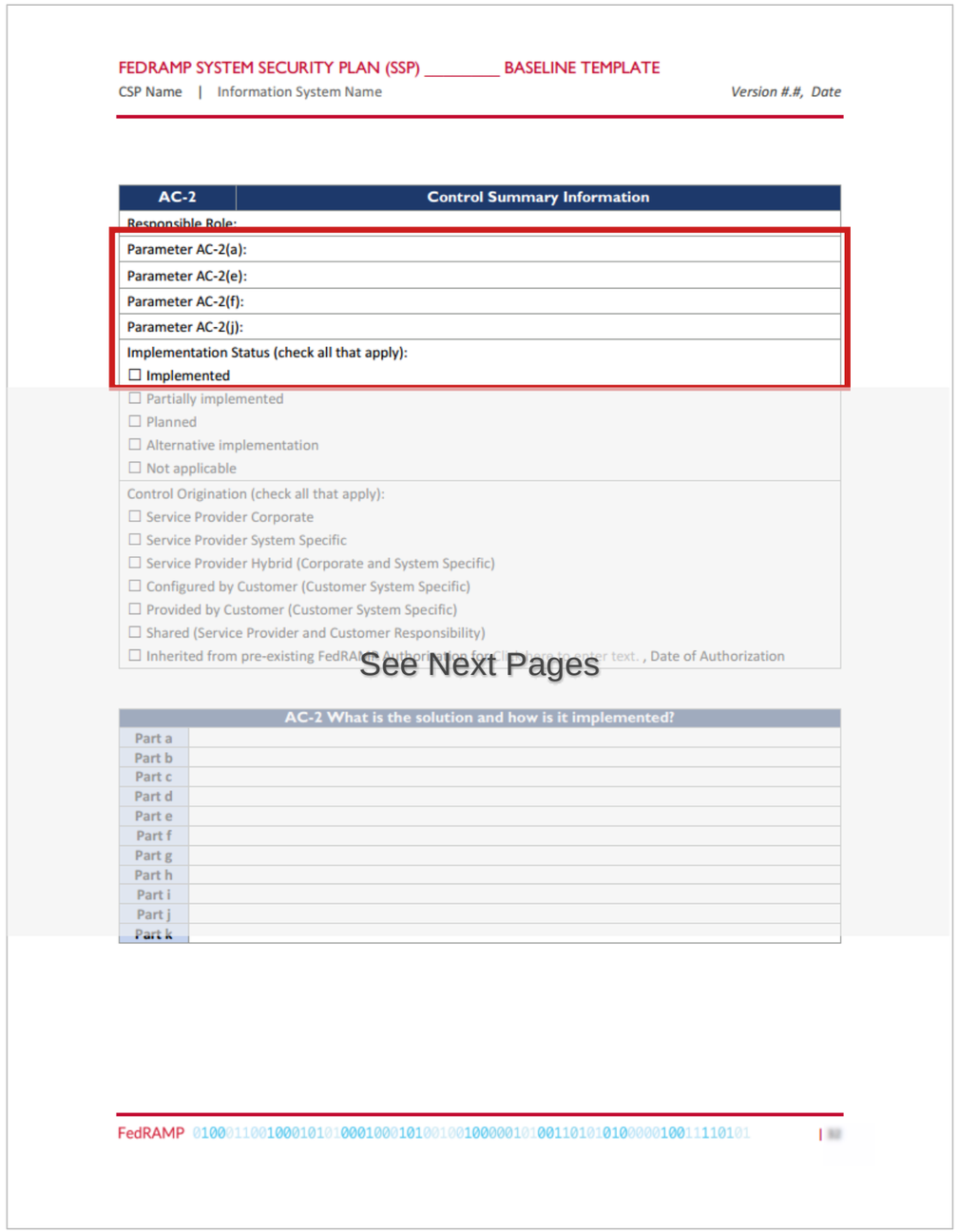
```
<!-- metadata -->
<import-profile href="https://path/to/xml/FedRAMP_MODERATE-baseline_profile.xml"/>
<!-- system-characteristics -->
<!-- system-implementation -->
<control-implementation>
    <description>
        <p>This field required by OSCAL, but may be left blank.</p>
        <p>FedRAMP requires no specific content here.</p>
    </description>

    <!-- one implemented-requirement assembly for each required control -->
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <!-- Control content cut - See next pages for detail -->
    </implemented-requirement>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
    <!-- Control content cut - See next pages for detail -->
    </implemented-requirement>
    <implemented-requirement uuid="uuid-value" control-id="ac-2.1">
    <!-- Control content cut - See next pages for detail -->
    </implemented-requirement>

</control-implementation>
<!-- back-matter -->
```

XPath Queries

```
URI to Profile:
  /*/import-profile/@href

CSP's Control Implementation Information
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]
```

Replace "ac-1" with target control ID.

NOTE: FedRAMP tools check to ensure there is one `implemented-requirement` assembly for each control identified in the applicable FedRAMP baseline.



6.2 Responsible Roles and Parameter Assignments

Every applicable control must have at least one `responsible-role` defined. There must be a separate `responsible-role` assembly for each responsible role. OSCAL requires the specified `role-id` to be valid in the defined list of `roles` in the `metadata`. Controls with a FedRAMP `implementation-status` property value of `non-applicable` (see section 5.3) do not require a `responsible-role`. FedRAMP further requires the specified `role-id` must also have been referenced in the `system-implementation`/`user` assembly. This equates to the FedRAMP requirement of all responsible roles appearing in the Personnel Roles and Privileges table.

With the `implemented-requirement` assembly, there must be one `set-parameter` statement for each of the control's parameters, as specified in the FedRAMP baseline and illustrated in the example representation below. The only exception to this is with nested parameters. Some select parameters contain an assignment parameter within a selection parameter, such as appears in AC-7 (b). In these instances, only the final selected value must be provided. The nested assignment parameter may be ignored.

OSCAL also supports parameter setting at the component level, within a `by-component` assembly.

Representation

```
<metadata>
    <role id="admin-unix">
        <title>Unix Administrator</title>
    </role>
</metadata>
<!-- Fragment: -->
<system-implementation>
    <user uuid="uuid-value">
        <role-id>admin-unix</role-id>
    </user>
</system-implementation >
<!-- system-implementation -->
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <!-- cut -->
        <responsible-role role-id="admin-unix" />
        <set-parameter param-id="ac-2_prm_1">
            <value>System Manager, System Architect, ISSO</value>
        </set-parameter >
        <!-- cut -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

```
Number of specified Responsible Roles:
  count(/*/control-implementation/implemented-requirement[@control-id="ac-2"]/
  responsible-role)
```

Replace "ac-2" with target control ID.

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

```
Responsible Role:
  /*/metadata/role[@id=/*/control-implementation/implemented-requirement
  [@control-id="ac-2"]/responsible-role[1]/@role-id]/title

Check for existence in Personnel Roles and Privileges (Should return a number > 0)
  count(/*/system-implementation/user/role-id[string(.)=/*/control-implementation/
  implemented-requirement[@control-id="ac-2"]/responsible-role/@role-id])

Parameter Value:
  /*/control-implementation/implemented-requirement[@control-id="ac-2"]/set-parameter
  [@param-id="ac-2_prm_1"]/value
```

Replace "ac-2_prm_1" with target parameter ID.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	

See Previous Page

Implementation Status (check all that apply):

- ☐ Implemented
- ☐ Partially implemented
- ☐ Planned
- ☐ Alternative implementation
- ☐ Not applicable

Control Origination (check all that apply):

- ☐ Service Provider Corporate
- ☐ Service Provider System Specific
- ☐ Service Provider Hybrid (Corporate and System Specific)
- ☐ Configured by Customer (Customer System Specific)
- ☐ Provided by Customer (Customer System Specific)
- ☐ Shared (Service Provider and Customer Responsibility)
- ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization

See Next Pages

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	

FedRAMP Extensions and Accepted Values

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

- `name="planned-completion-date"`

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

- `name="implementation-status"`
  Valid: `implemented, partial, planned, alternative, not-applicable`

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

6.3 Implementation Status

FedRAMP only accepts only one of five values for `implementation-status`: `implemented`, `partial`, `planned`, `alternative`, and `not-applicable`. A control may be marked “partial” and “planned” (using two separate `implementation-status` fields). All other choices are mutually exclusive.

If the implementation-status is `partial`, the gap must be explained in the `remarks` field.

If the implementation-status is `planned`, a brief description of the plan to address the gap, including major milestones must be explained in the `remarks` field. There must also be a prop (`name="planned-completion-date" ns="https://fedramp.gov/ns/oscal"`) field containing the intended completion date. With XML, prop fields must appear before `prop` fields, even though that sequence is counter-intuitive in this situation.

If the implementation-status is `alternative`, the alternative implementation must be summarized in the `remarks` field.

If the implementation-status is `not-applicable`, the N/A justification must be provided in the `remarks` field.

Implementation Status Representation

```
<!-- system-implementation -->
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <prop name="planned-completion-date"
            ns="https://fedramp.gov/ns/oscal" value="2021-01-01Z"/>
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="implemented" />
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="partial" />
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="planned" />
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="not-applicable"/>
        <!-- responsible-role, statement, by-component -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

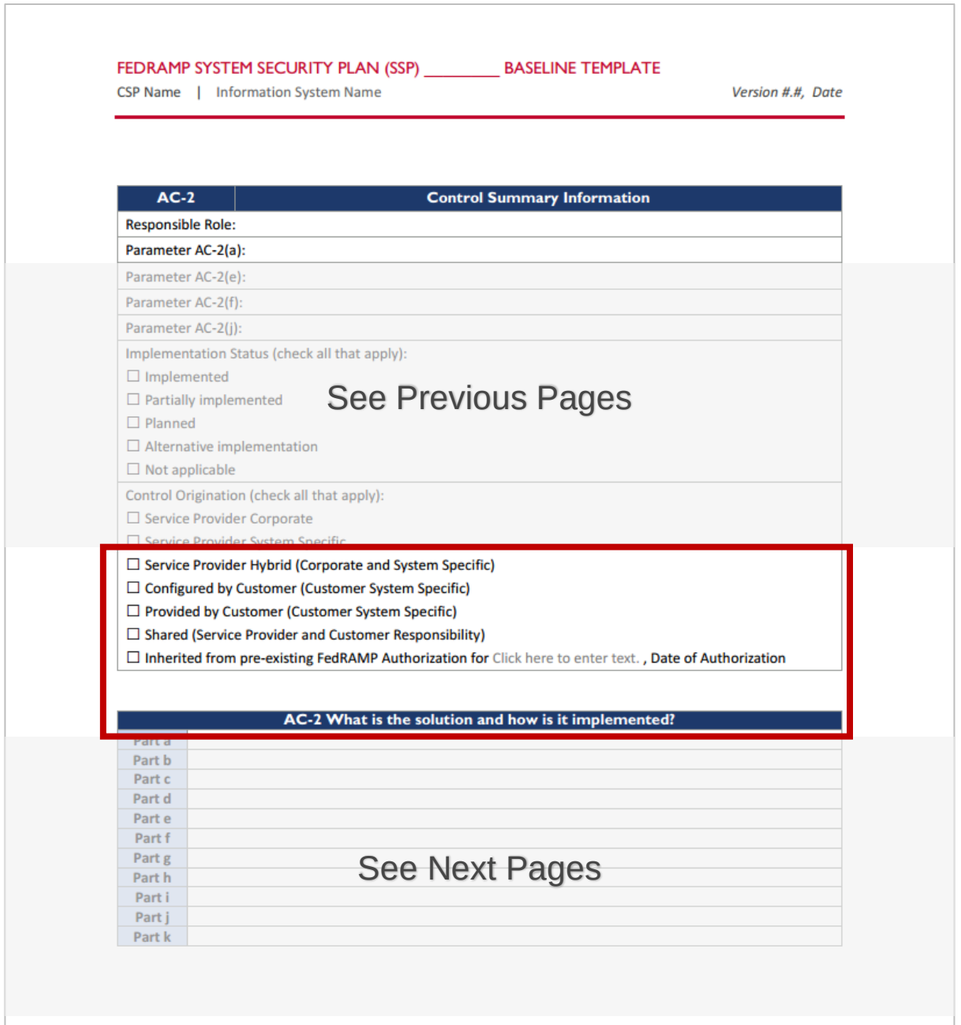
Implementation Status XPath Queries

Replace "ac-1" with target control-id.

```
Implementation Status (may return more than 1 result for a given control):
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]
  /prop[@name="implementation-status"]/@value

Gap Description (If implementation-status="partial"):
  /*/control-implementation/implemented-requirement/prop[@name='implementation-
  status'][@value="partial"][@ns="https://fedramp.gov/ns/oscal"]/remarks/node()

Planned Completion Date (If implementation-status="planned"):
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]/
  prop[@name="planned-completion-date"][@ns="https://fedramp.gov/ns/oscal"]/@value

Plan for Completion (If implementation-status="planned"):
  /*/control-implementation/implemented-requirement/prop[@name='implementation-
  status'][@value="planned"][@ns="https://fedramp.gov/ns/oscal"]/remarks/node()
```

```
Not Applicable (N/A) Justification (If implementation-status="na"):
  /*/control-implementation/implemented-requirement/prop[@name='implementation-
  status'][@value="not-applicable"][@ns="https://fedramp.gov/ns/oscal"]/remarks/node()
```

The FedRAMP `implementation-status` property at the control's `implemented-requirement` level is a summary of all statement and/or component level core OSCAL `implementation-status` designations. It must be set to the appropriately based on the least value of child statement or component level `implementation-status` designations. When a statement and/or component level `implementation-status` designation is not specified, the FedRAMP `implementation-status` value is assumed. Individual statements and/or components may override `implementation-status` locally.


FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	See Previous Pages
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	
AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

See Next Pages

FedRAMP Extensions and Accepted Values

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

- `name="control-origination"`
  Valid: `sp-corporate`, `sp-system`, `customer-configured`, `customer-provided`, `inherited`

Instead of hybrid, identify multiple control-origination types, each in its own `prop` assembly.

6.3.1.1 Control Origination

FedRAMP accepts only one of five values for `control-origination`: `sp-corporate`, `sp-system`, `customer-configured`, `customer-provided`, and `inherited`. Hybrid choices are now expressed by identifying more than one `control-origination`, each in a separate prop field.
For controls with a control-id ending in "-1", FedRAMP only accepts `sp-corporate`, and `sp-system`.

If the control origination is `inherited`, there must also be a FedRAMP extension (`prop name="leveraged-authorization-uuid" ns="https://fedramp.gov/ns/oscal"`) field containing the UUID of the leveraged authorization as it appears in the `/*/system-implementation/leveraged-authorization` assembly.

Control Origination Representation

```
<system-implementation>
    <!-- status -->
    <leveraged-authorization uuid="uuid-of-leveraged-authorization">
        <!-- details cut - see Leveraged Authorizations Section -->
    </leveraged-authorization>
</system-implmentation>

<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <prop name="leveraged-authorization-uuid"
            value="uuid-of-leveraged-authorization"/>
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="sp-corporate" />
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="sp-system" />
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="customer-configured" />
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="inherited" />
        <!-- responsible-role -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

```
Number of Control Originations:
  count(/*/control-implementation/implemented-requirement[@control-id="ac-2"]/
  prop[@name="control-origination"][@ns="https://fedramp.gov/ns/oscal"])

Control Origination(could return more than 1 result):
  /*/control-implementation/implemented-requirement[@control-id="ac-2"]/prop
  [@name="control-origination"][@ns="https://fedramp.gov/ns/oscal"][1]/@value

Inherited From: System Name (If control-origination="inherited"):
  /*/system-implementation/leveraged-authorization[@uuid=/*/control-implementation/
  implemented-requirement[@control-id="ac-2"]/prop[@name="leveraged-authorization-
  uuid"]]/title

Inherited From: Authorization Date (If control-origination="inherited"):
  /*/system-implementation/leveraged-authorization[@uuid=/*/control-implementation/
```

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

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

```
implemented-requirement[@control-id="ac-2"]/prop[@name="leveraged-authorization-uuid"]]/date-authorized
```

Policy and Procedure Statements

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AC-1 What is the solution and how is it implemented?	
Part a	
Part b1	
Part b2	

Multi-Part Statements

The organization:

(a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

(b) Assigns account managers for information system accounts;

cut c, d, e, f, g, h, i

(j) Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: monthly for privileged accessed, every six (6) months for non-privileged access*]; and

(k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

Single Statement

The organization employs automated mechanisms to support the management of information system accounts.

AC-2 (1) What is the solution and how is it implemented?

6.4 Control Implementation Descriptions

Within the OSCAL-based FedRAMP baselines, control statements and control objectives are tagged with a `response-point` FedRAMP Extension. Every control statement designated as a `response-point` in the baseline must have a `statement` with the control's `implemented-requirement` assembly. Please note control objective response points are used for the SAP and SAR.

When using a **FedRAMP Resolved Profile Catalog**, the following query will identify the response points for a given control.

XPath Query

```
Response Points for AC-1:
  //control[@id='ac-1']/part[@name='statement']//prop[@na
  point'][@ns='https://fedramp.gov/ns/oscal']/../@id
```

Replace "ac-1" with other control IDs as required.

6.4.1 Organization: Policy and Procedure Statements

For each of the -1 controls, such as AC-1, there must be exactly four `statement` assemblies: Part (a)(1), Part (a)(2), Part (b)(1), and Part (b)(2).

Policy and Procedure Representation

```
<!-- system-implementation -->
<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <statement statement-id="ac-1_smt.a.1"><!-- cut --></statement>
        <statement statement-id="ac-1_smt.a.2"><!-- cut --></statement>
        <statement statement-id="ac-1_smt.b.1"><!-- cut --></statement>
        <statement statement-id="ac-1_smt.b.2"><!-- cut --></statement>
    </implemented-requirement>
</control-implementation>
```

6.4.2 Organization: Multi-Part Statements:

There must be one `statement` assembly for each lettered part, such as with AC-2, parts a, b, c, etc.

Multi-Part Statement Representation

```
<!-- system-implementation -->
<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement statement-id="ac-2_smt.a"><!-- cut --></statement>
        <!-- repeat for b, c, d, e, f, g, h, i, j -->
        <statement statement-id="ac-2_smt.k"><!-- cut --></statement>
    </implemented-requirement>
</control-implementation>
```

See Previous Pages

6.4.3 Organization: Single Statement

If there are no lettered parts in the control definition, such as with AC-2 (1), there must be exactly one `statement` assembly.

Single-Statement Representation

```
<!-- system-implementation -->
<control-implementation>
    <!-- cut -->
    <implemented-requirement control-id="ac-2.1">
        <statement statement-id="ac-2.1_smt"><!-- cut --></statement>
    </implemented-requirement>
</control-implementation>
```

6.4.4 Response: Overview

Within each `statement` assembly, all responses must be provided within one or more `by-component` assemblies. There must always be a component defined in the `system-implementation` representing the system as a whole (**"THIS SYSTEM"**), even if individual components are defined that comprise the system. **See *7.3, Working with Components* for more information.**

An OSCAL-based FedRAMP SSP should define individual components of the system. Components are not just hardware and software. Policies, processes, FIPS 140 validation information, interconnections, services, and underlying systems (leveraged authorizations) are all components.

With OSCAL, the content in the cell next to *Part a* must be broken down into its individual components and responded to separately.

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

COMPONENT APPROACH: AC-2 What is the solution and how is it implemented?

Part a

Component	Description
THIS SYSTEM	Describes how *part a* is satisfied holistically, or where the description does not fit with a defined component.
Platform	Describes how *part a* is satisfied by the platform.
Web-server	Describes how *part a* is satisfied by the web server
Process	Describes how *part a* is satisfied by an identified process within this organization.
Inherited	Describes what is inherited from the underlying Infrastructure as a Service (IaaS) provider to satisfy *part a*.

Part b

Component	Description
THIS SYSTEM	Describes how *part b* is satisfied holistically, or where the description does not fit with a defined component.
Platform	Describes how *part b* is satisfied by the platform.
Web-server	Describes how *part b* is satisfied by the web server
Process	Describes how *part b* is satisfied by an identified process within this organization.
Inherited	Describes what is inherited from the underlying Infrastructure as a Service (IaaS) provider to satisfy *part b*.

The following pages provide examples.

Converting Legacy SSPs to OSCAL

For CSPs converting their existing MS Word-based SSP to OSCAL, FedRAMP allows the entire part response to initially be associated with the **"THIS SYSTEM"** component. Once converted, the CSP is encouraged to begin defining individual components and move content from the general **"THIS SYSTEM"** description to the component-specific description.

See *7.4, Converting a Legacy SSP to OSCAL* for an alternative OSCAL control representation, which aligns better with legacy SSP content.

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

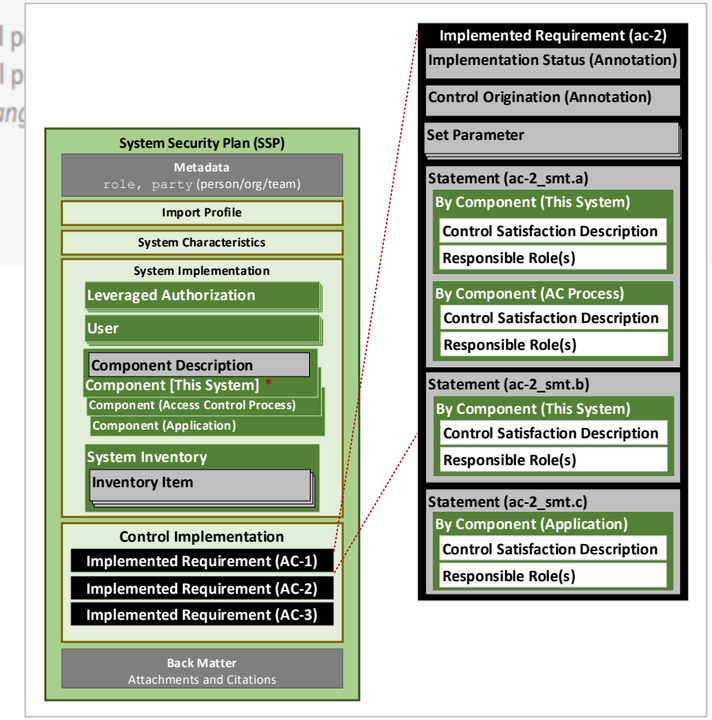
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

See Previous Pages

(b) Reviews and updates the current:

(1) Access control p

(2) Access control p
significant chang



The `description` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-

6.4.5 Response: Example

Within each of the `statement` assemblies, all responses appear in one or more `by-component` assemblies. Each `by-component` assembly references a `component` defined in the `system-implementation` assembly.

Representation

```
<system-implementation>
    <!-- leveraged-authorization, user -->
    <component uuid="uuid-value" type="software">
        <title>Component Title</title>
        <description>
            <p>Description of the component.</p>
        </description>
        <status state="operational"/>
    </component>

    <component uuid="uuid-value" type="process">
        <title>Process Title</title>
        <description>
            <p>Description of the component.</p>
        </description>
        <status state="operational"/>
        <responsible-role role-id="admin-unix">
            <party-uuid>3360e343-9860-4bda-9dfc-ff427c3dfab6</party-uuid>
        </responsible-role>
    </component>
</system-implementation>

<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2 smt.a">

            <by-component uuid="uuid-value" component-uuid="uuid-of-software-component">
                <description>
                    <p>Describe how is the software component satisfying the control.</p>
                </description>
            </by-component>
            <by-component uuid="uuid-value" component-uuid="uuid-of-process-component">
                <description>
                    <p>Describe how is the process satisfies the control.</p>
                </description>
            </by-component>
            <!-- repeat by-component assembly for each component related to part a. -->

        </statement>
        <!-- repeat statement assembly for statement part (b, c, etc.) as needed. -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

See Section 6.4.10, XPath Queries for Control Implementation Descriptions

NOTES:

- All `statement-id` values must be cited as they appear in the NIST SP 800-53, Revision 4 or Revision 5 OSCAL catalogs: https://github.com/usnistgov/oscal-content/tree/master/nist.gov/SP800-53

When converting a legacy SSP to OSCAL, the legacy content can be associated with the "This System" component until the SSP author is able to provide more granular content.

13.1. Access Control (AC)

AC-1 Access Control Policy and Procedures Requirements (H)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AC-1	Control Summary Information
Responsible Role:	
Parameter AC-1(a):	
Parameter AC-1(b)(1):	
Parameter AC-1(b)(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

AC-1 What is the solution and how is it implemented?	
Part a	
Part b1	
Part b2	

6.4.6 Response: "This System" Component

There must always be a **"This System"** component in the SSP. This is used in several ways:

- **Holistic Overview**: If the SSP author wishes to provide a more holistic overview of how several components work together, even if details are provided individually in other `by-component` assemblies.
- **Catch-all**: Any control response that does not cleanly align with another system component may be described in the **"This System"** component.
- **Legacy SSP Conversion**: When converting a legacy SSP to OSCAL, the legacy control response statements may initially be associated with the **"This System"** component until the SSP author is able to provide responses for individual components.

Representation

```
<system-implementation>
    <!-- leveraged-authorization, user -->
    <component uuid="uuid-value" type="this-system">
        <title>This System</title>
        <description>
            <p>Description of the component.</p>
        </description>
        <status state="operational"/>
    </component>
</system-implementation>

<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2_smt.a">

            <by-component uuid="uuid-value" component-uuid="uuid-of-this-system-component">
                <description>
                    <p>Describe how individual components are working together.</p>
                    <p>Describe how the system - as a whole - is satisfying this
statement.</p>
                    <p>This can include policy, procedures, hardware, software, etc.</p>
                </description>
            </by-component>

        </statement>
        <!-- repeat statement assembly for statement part (b, c, etc.) as needed. -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

See Section 6.4.10, XPath Queries for Control Implementation Descriptions

NOTES:

- Although the name of the component is **"This System"**, non-technical solutions may also be discussed here, such as policies and procedures.

AC-1 Access Control Policy and Procedures Requirements (H)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AC-1	Control Summary Information
Responsible Role:	
Parameter AC-1(a):	
Parameter AC-1(b)(1):	
Parameter AC-1(b)(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

AC-1 What is the solution and how is it implemented?	
Part a	
Part b1	
Part b2	

6.4.7 Linking to Artifacts

Any time policies, procedures, plans, and similar documentation are cited in a control response, they must be linked.

For the legacy approach, when responding within the by-component assembly for **"this system"**, the link must be within the same by-component assembly where the artifact is cited.

Representation: Legacy Approach Example - No Policy Component

```
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <statement uuid="uuid-value" statement-id="ac-1_smt.a">
            <by-component component-uuid="uuid-of-this-system" uuid="uuid-value">
                <description>
                    <p>Describe how Part a is satisfied within the system.</p>
                </description>
                <link href="#uuid-of-policy-resource-in-back-matter" rel="policy" />
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

For the component approach, use the component representing the policy. The link should be in the component, but may be added directly to the by-component as well.

Representation: Component Approach Example

```
<system-implementation>
    <!-- leveraged-authorization, user -->
    <component uuid="uuid-value" type="policy">
        <title>Access Control and Identity Management Policy</title>
        <description>
            <p>An example component representing a policy.</p>
        </description>
        <link href="#uuid-of-policy-resource-in-back-matter" rel="policy" />
        <status state="operational"/>
    </component>
</system-implementation>
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <statement uuid="uuid-value" statement-id="ac-1_smt.a">
            <by-component component-uuid="uuid-of-policy-component" uuid="uuid-value">
                <description>
                    <p>Describe how this policy satisfies Part a.</p>
                </description>
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

When a responsibility is linked to a provided assembly it indicates to a leveraging system that if inheritance is desired, the customer responsibility must be satisfied. If the leveraging system elects to ignore inheritance and implement their own solution, the linked responsibility may be ignored.

If a responsibility is always required, add it to the by-component assembly representing **"this system"** and do not link it to a provided assembly.

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/reference/datatypes/

For either example above, the policy must be present as a `resource` in `back-matter`.

In Back Matter

```
<back-matter>
    <resource uuid="uuid-value">
        <title>Access Control and Identity Management Policy</title>
        <rlink media-type="application/pdf" href="./documents/policies/sample_policy.pdf" />
        <base64 filename="sample_policy.pdf" media-type="application/pdf">00000000</base64>
    </resource>
</back-matter>
```

6.4.8 Response: Identifying Inheritable Controls and Customer Responsibilities

For systems that may be leveraged, OSCAL enables a robust mechanism for providing both inheritance details as well as customer responsibilities (referred to as consumer responsibilities by NIST). OSCAL is designed to enable leveraged and leveraging system SSP details to be linked by tools for validation.

Within the appropriate `by-component` assembly, include an `export` assembly. Use `provided` to identify a capability that may be inherited by a leveraging system. Use `responsibility` to identify a customer responsibility. If a responsibility must be satisfied to achieve inheritance, add the `provided-uuid` flag to the `responsibility` field.

Representation

```
<!-- system-implementation -->
<control-implementation><!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2_smt.a">
            <by-component uuid="uuid-value" component-uuid="uuid-of-this-system-component">
                <description>
                    <p>Describe how the system - as a whole - is satisfying this
statement.</p>
                </description>
                <export>
                    <responsibility uuid="uuid-value">
                        <description>
                            <p>Leveraging system's responsibilities in satisfaction of AC-
2.</p>
                            <p>Not linked to inheritance, so this is always required.</p>
                        </description>
                        <responsible-role role-id="customer" />
                    </responsibility>
                </export>
            </by-component>
            <by-component uuid="uuid-value" component-uuid="uuid-of-software-component">
                <description>
                    <p>Describe how the software is satisfying this statement.</p>
                </description>
```

```
                <export>
                    <provided uuid="uuid-value">
                        <description>
                            <p>Customer appropriate description of what may be inherited.</p>
                        </description>
                        <responsible-role role-id="poc-for-customers" />
                    </provided>

                    <responsibility uuid="uuid-value" provided-uuid="uuid-of-provided">
                        <description>
                            <p>Customer responsibilities if inheriting this capability.</p>
                        </description>
                        <responsible-role role-id="customer" />
                    </responsibility>
                </export>
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
```

See Section 6.4.10, XPath Queries for Control Implementation Descriptions

See the NIST OSCAL Leveraged Authorization Presentation for more information.

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

The `provided-uuid` flag in `inherited` links to the provided statement in the leveraged system's SSP.

The `responsibility-uuid` flag in satisfied links to the `responsibility` statement in the leveraged system's SSP.

Both may be exposed to the leveraging system via the OSCAL Inheritance and Responsibility model when the leveraging system owner is not entitled to see the leveraged system's SSP as is typical with FedRAMP-authorized systems. This model replaces the CRM.

The `description` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

6.4.9 Leveraged Authorization Response: Inheriting Controls, Satisfying Responsibilities

When the current system is inheriting a control from or meeting customer responsibilities defined by an underlying authorization, the leveraged system must first be defined as described in *Section **Error! Reference source not found.**, **Error! Reference source not found.*** before it may be referenced in a control response. The `by-component` assembly references these components.

IMPORTANT: The leveraged system may provide a single component representing the entire leveraged system or may provide individual system components as well. In either case, the `inherited-uuid` property in the component when defined in the leveraging system's SSP.

Representation

```
<system-implementation>
    <component uuid="uuid-value" type="this-system"><!-- cut --></component>
    <component uuid="uuid-value" type="leveraged-system">
        <title><b>LEVERAGED SYSTEM as a whole (IaaS)</b></title>
        <prop name="leveraged-authorization-uuid" value="uuid-of-LA-in-this-SSP" />
        <prop name="inherited-uuid" value="uuid-of-component-in-leveraged-SSP" />
    </component>
    <component uuid="uuid-value" type="service">
        <title>Service Provided by Leveraged System</title>
        <prop name="leveraged-authorization-uuid" value="uuid-of-LA-in-this-SSP" />
        <prop name="inherited-uuid" value="uuid-of-component-in-leveraged-SSP" />
    </component>
</system-implementation>
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2_smt.a">
            <by-component uuid="uuid-value" component-uuid="uuid-of-this-system-component">
                <description><p>Describe what is satisfied by this system.</p></description>
            </by-component>

            <by-component uuid="uuid-value" component-uuid="uuid-leveraged-system-component">
                <description>
                    <p>Describe what is inherited from the leveraged system in satisfaction
                        of this control statement.</p>
                </description>

                <inherited provided-uuid="uuid-of-provided" uuid="uuid-value">
                    <description>
                        <p>Optional: Information provided by leveraged system.</p>
                    </description>
                </inherited>

                <satisfied responsibility-uuid="uuid-of-responsibility" uuid="uuid-value" >
                    <description>
                        <p>Description of how the responsibility was satisfied.</p>
                    </description>
                </satisfied>
            </by-component>
```

The `description` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-

```
        </statement>
        <!-- repeat statement assembly for statement part (b, c, etc.) as needed. -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

See Section 6.4.10, XPath Queries for Control Implementation Descriptions

See the NIST OSCAL Leveraged Authorization Presentation for more information.

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and

(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

See Previous Pages

6.4.10 XPath Queries for Control Implementation Descriptions

Use the following XPath queries to retrieve basic control response information. For any given control response part, tools should list the name of each component cited by a `by-component` assembly, as well as the description.

XPath Queries

```
Number of cited components for AC-2, part a (Integer):
  count(/*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-component)

Name of first component related to AC-2, part a:
  /*/system-implementation/component[@uuid=/*/control-implementation/implemented-
  requirement[@control-id="ac-2"]/statement[@statement-id="ac-2_smt.a"]/by-
  component[1]/@component-uuid]/title

"What is the solution and how is it implemented?" for AC-2, Part (a), first component:
  /*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-component[1]/description/node()

Is there a customer responsibility for the first component in AC-2, part a?
  (true/false):
  boolean(/*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-component[1]
  /prop[@name='responsibility'][@value='customer'])

Customer responsibility statement for the first component in AC-2, part a:
  /*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-
  component[1]/prop[@name='responsibility'][@value='customer']/remarks/node()
```

NOTES:

- Replace “ac-2” with target control-id.
- Replace “ac-2_smt.a” with target control statement-id.
- Replace '”1]” with “[2]”, “[3]”, etc. as needed to reference is by-component statement.

7 Generated Content

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

- **Control Information Summary (CIS)**
- **Customer Responsibility Matrix (CRM)**

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

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

7.1 Generating the Control Information Summary (CIS)

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

https://github.com/GSA/fedramp-automation/tree/master/dist/content/rev5/resources

7.2 Generating the Customer Responsibility Matrix (CRM)

There are many ways a tool developer can generate the CRM. FedRAMP is developing an XSLT file to generate the FedRAMP CRM. When ready, FedRAMP will make this freely available to the public here:

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

Useful CRM XPath Queries

```
Flat-File CRM Query:
  //control-implementation/implemented-requirement/prop[@name="control-
  origination"][@ns="https://fedramp.gov/ns/oscal"][@value="customer-
  configured" or @value="customer-provided"]/remarks/node()

Component-based CRM Query:
  //control-implementation/implemented-requirement/statement/by-component
  [@component-id="customer"]/description
```

7.3 Working with Components

NIST designed OSCAL such that a system architect can express all aspects of the system as components. A component is anything that can satisfy a control requirement. This includes hardware, software, services, and underlying service providers, as well as policies, plans, and procedures. There are several ways to use components in an OSCAL-based SSP. The following defines FedRAMP's minimum initial use.

Anything that can satisfy a control requirement is a component, including hardware, software, services, policies, plans, and procedures.

This section will likely be updated as NIST continues to evolve its approach to components in OSCAL, and as FedRAMP receives feedback from stakeholders.

FedRAMP-defined component identifiers are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

7.3.1 Minimum Required Components

There must be a component that represents the entire system itself. It should be the only component with the `component-type` set to "`system`".

The following is an example of defined components.

Minimum Required Component Representation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->

    <!-- This System -->
    <component uuid="uuid-value" type="this-system" >
        <title>This System</title>
        <description><p>
            The entire system as depicted in the system authorization boundary.
        </p></description>
        <status state="operational" />
    </component>

</system-implementation>
```

NIST has clarified the approach to leveraged authorizations and the CRM. Leveraged authorizations and customer responsibility content are no longer handled as components. These scenarios require special handling as described in Section6, Attachments

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The resource's `title` and `description` must be used to provide a human-readable indicator of what

7.3.2 Common Additional Components

For each FIPS 140 validated module, there must be a component that represents the validation certificate itself. For more information about this, see the *FIPS 140 Validated Components* Section.

Common Additional Component Representation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->
    <!-- System Component -->

    <!-- Ports, Protocols and Services Entry -->
    <component uuid="uuid-of-service" type="service">
        <title>[SAMPLE]Service Name</title>
        <description><p>Describe the service</p></description>
        <purpose>Describe the purpose the service is needed.</purpose>
        <prop name="used-by" value="What uses this service?"/>
        <status state="operational" />
        <protocol name="http">
            <port-range start="80" end="80" transport="TCP"/>
        </protocol>
        <protocol name="https">
            <port-range start="443" end="443" transport="TCP"/>
        </protocol>
    </component>

    <!-- FIPS 140 Validation Certificate Information -->
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="validation">
        <title>Module Name</title>
        <description><p>FIPS 140 Validated Module</p></description>
        <prop name="validation-type" value="fips-140-2"/>
            <prop name="validation-reference" value="0000"/>
            <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" />
            <status state="operational" />
    </component>

    <!-- service -->
</system-implementation>
<!-- control-implementation -->
```

NIST has clarified the approach to leveraged authorizations and the CRM. Leveraged authorizations and customer responsibility content are no longer handled as components. These scenarios require special handling as described in Section 6, Attachments

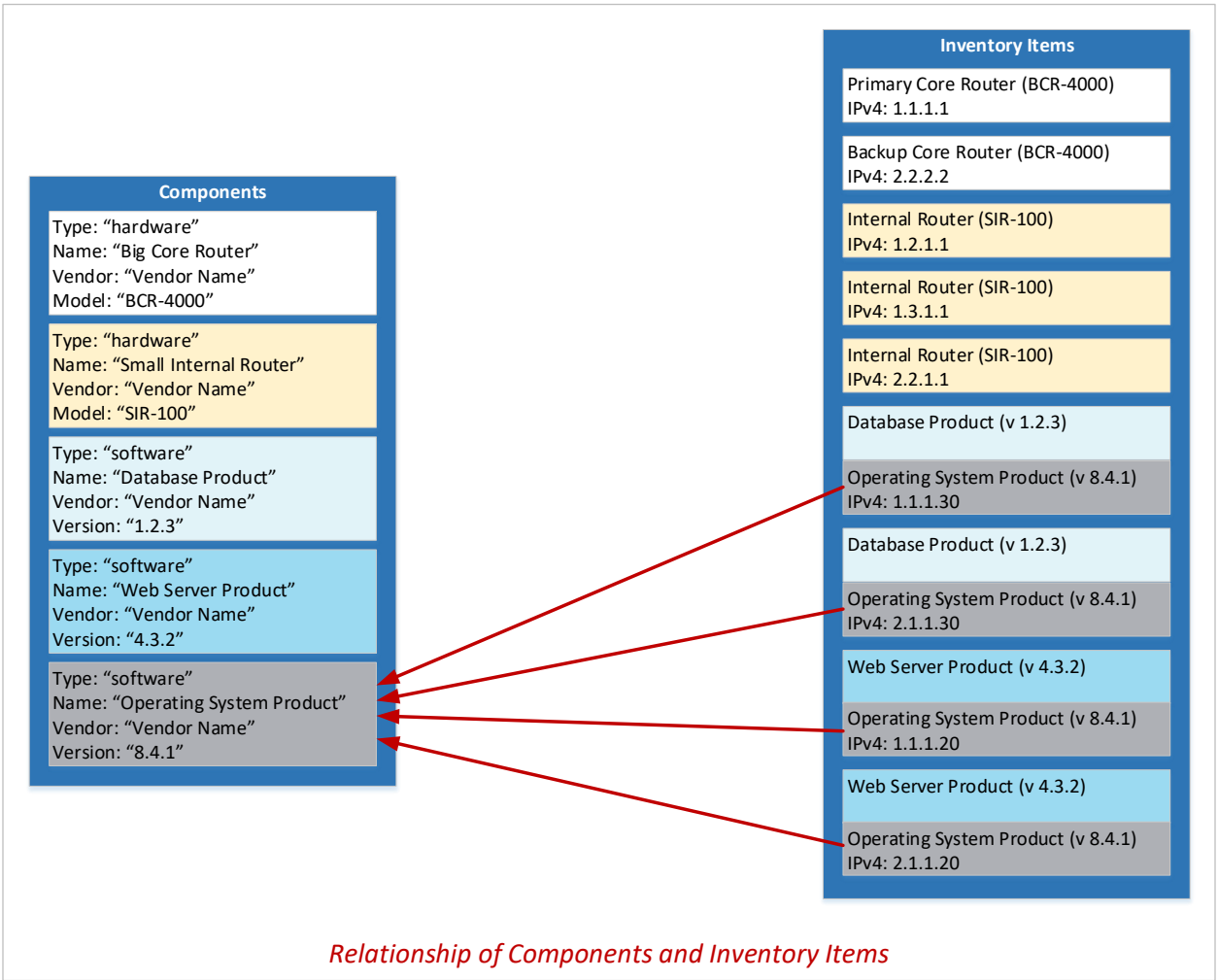
Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The resource's `title` and `description` must be used to provide a human-readable indicator of what attachment is being referenced, however, OSCAL extensions must also be provided when applicable for machine

7.3.3 Components as a Basis for System Inventory

NIST's approach to component-based system modeling is to reduce redundancy of information and increase flexibility. NIST accomplishes this with separate component and inventory item modeling.

This is a one-to-many relationship. One component to many inventory item instances.

For example, if an open-source operating system (OS) is used in many places throughout the system, it is defined once as a component. All information about the product, vendor, and support are modeled within the component detail. If the OS is used four times within the system, each use is an inventory item, with details about that specific information, such as IP address.



Relationship of Components and Inventory Items

FedRAMP requires a component assembly for each model of infrastructure device used, and each version of software and database used within the system. FedRAMP is not asking for

more detail than provided in the legacy inventory workbook. Only that the information is organized differently.

As NIST continues to evolve its component approach, FedRAMP will re-evaluate its approach to system inventory representation.

7.4 Converting a Legacy SSP to OSCAL

NIST designed OSCAL such that a system architect can express all aspects of the system as components. A component is anything that can satisfy a control requirement. This includes hardware, software, services, and underlying service providers, as well as policies, plans, and procedures.

OSCAL is also designed to support legacy conversion of SSPs without individual components defined and enables an SSP author to migrate to the component approach gradually over time. In this instance, only a single component is initially required, representing the system as a whole and designated with the special component type, "`this-system`". The following provides an example of FedRAMP's minimum required component approach:

Anything that can satisfy a control requirement is a component, including hardware, software, services, policies, plans, and procedures.

Example control for legacy SSP conversion

```
<!-- system-characteristics -->
<system-implementation>
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="this-system">
        <title>System Name</title>
        <description>
            <p>Component representing the entire system.</p>
        </description>
    </component>
</system-implementation>
<control-implementation>
    <description><p>FedRAMP SSP Template Section 13</p></description>
    <implemented-requirement control-id="ac-1" uuid="uuid-value">
        <statement statement-id="ac-1_stmt.a" uuid="uuid-value">
            <by-component component-uuid="Component-uuid-value" uuid="uuid-
value">
                <description>
                    <p>Describe how Part a is satisfied within the system.</p>
                </description>
            </by-component>
        </statement>
        <statement statement-id="ac-1_stmt.b.1" uuid="uuid-value">
            <by-component component-uuid="Component-uuid-value" uuid="uuid-
```

```
value">
                <description>
                    <p>Describe how Part b 1 is satisfied within the system.</p>
                </description>
            </by-component>
        </statement>
        <statement statement-id="ac-1_stmt.b.2" uuid="uuid-value">
            <by-component component-uuid="Component-uuid-value" uuid="uuid-
value">
                <description>
                    <p>Describe how Part b 2 is satisfied within the system.</p>
                </description>
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
```