DRAFT

GUIDE TO OSCAL-BASED FEDRAMP SECURITY ASSESSMENT REPORTS (SAR)

Version 1.0

June 1, 2020

FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
6/1/2020	Initial Publication	1.0	FedRAMP PMO
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to Contact Us

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

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

TABLE OF CONTENTS

1. OVERVIEW

1.1. Who Should Use This Document?

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

It provides guidance and examples intended to guide an organization in the production and use of OSCAL-based FedRAMP-compliant SAR files. Our goal is to enable your organization to develop tools that will seamlessly ensure these standards are met so your security practitioners can focus on SAR content and accuracy rather than formatting and presentation.

1.2. Related Documents

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

This document does not stand along. It provides information specific to developing tools to create and manage OSCAL-based, FedRAMP-compliant Security Assessment Reports.

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

Also, the OSCAL-based FedRAMP SAR builds on the content expressed in the OSCAL-based FedRAMP Security Assessment Plan (SAP) and the OSCAL-based System Security Plan (SSP). As a result, this document contains several references to the *Guide to OSCAL-based Security Assessment Plans (SAP)*, and the *Guide to OSCAL-based System Security Plans (SSP)*.

1.3. Basic Terminology

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

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

These terms are used by NIST in the creation of OSCAL syntax.

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

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

2. FEDRAMP EXTENSIONS, CONFORMITY TAGS, DEFINED IDENTIFIERS, AND ACCEPTED VALUES

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

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

A summary of the FedRAMP extensions, conformity tags, defined identifiers, and accepted values appears in the FedRAMP OSCAL Registry.

As a result, FedRAMP-compliant OSCAL files are a combination of the core OSCAL syntax and extensions defined by FedRAMP. The *Guide to OSCAL-based FedRAMP Content* describes the concepts behind FedRAMP extensions, conformity tags, defined identifiers, and accepted values. The extensions related to the SAR are cited in this document in context of their use.

FedRAMP extensions, conformity tags, defined identifiers, and accepted values are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

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

3. WORKING WITH OSCAL FILES

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

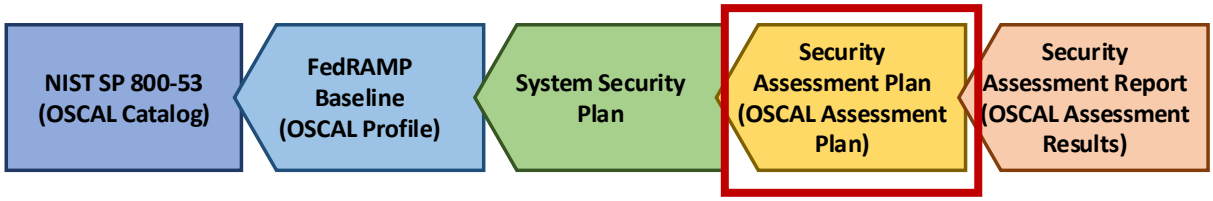
3.1. XML and JSON Formats

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

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

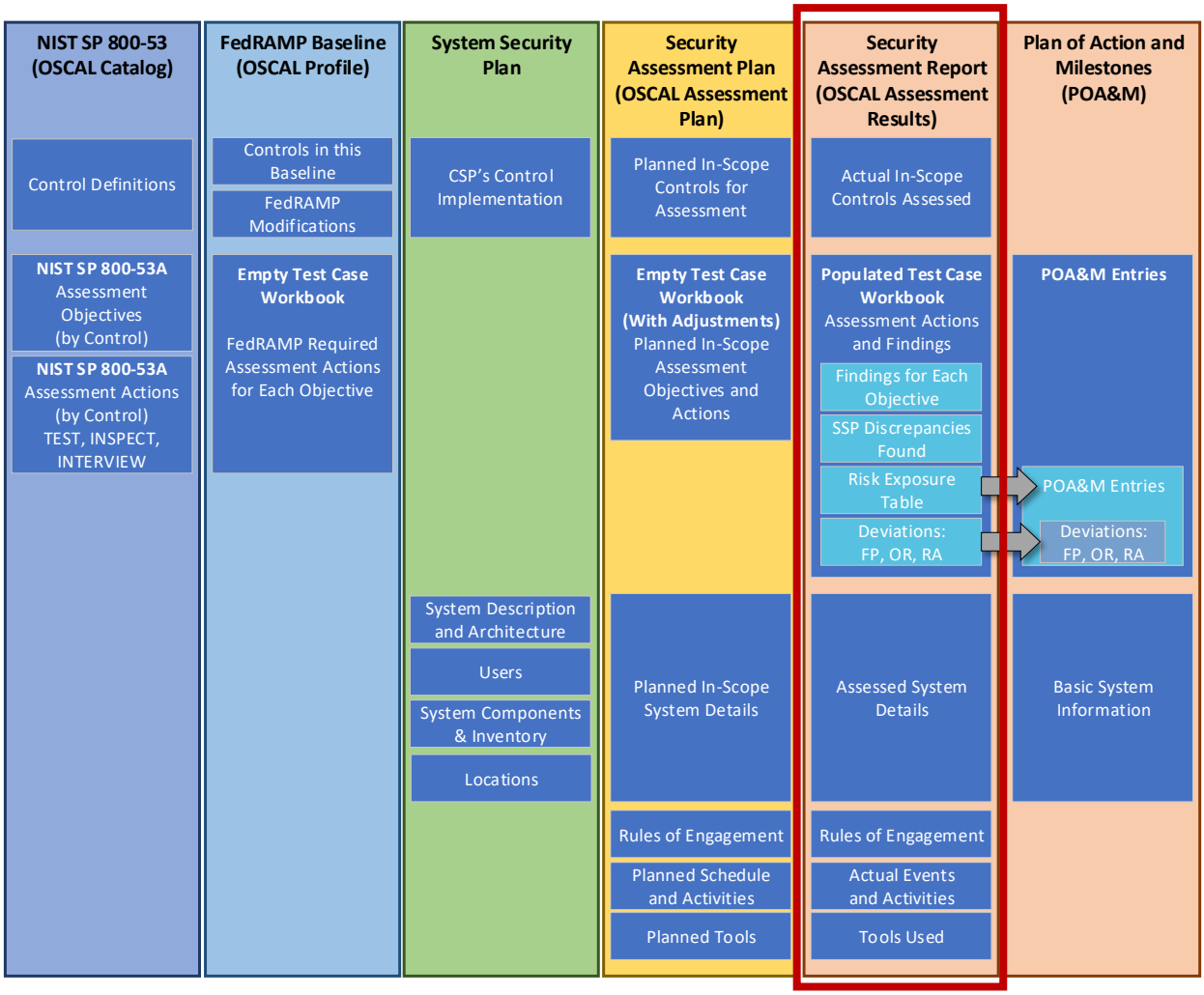
3.2. SAR File Concepts

Unlike the traditional MS Word-based SSP, SAP, and SAR, the OSCAL-based versions of these files are designed to make information available through linkages, rather than duplicating information. In OSCAL, these linkages are established through `import` commands.



Each OSCAL file imports information from the one before it

For example, the assessment objectives and actions that appear in a blank test case workbook (TCW), are defined in the FedRAMP profile, and simply referenced by the SAP and SAR. Only deviations from the TCW are captured in the SAP or SAR.



Baseline and SSP Information is referenced instead of duplicated.

For this reason, an OSCAL-based SAR points to the OSCAL-based SAP for this assessment. In turn, the SAP points to the OSCAL-based SSP of the system being assessed. Instead of duplicating system details,

the OSCAL-based SAR simply points to the SSP content (via the SAP) for information such as system description, boundary, users, locations, and inventory items.

The SAR also inherits the SSP's pointer to the appropriate OSCAL-based FedRAMP Baseline via the SAP. Through that linkage, the SAR references the assessment objectives and actions typically identified in the FedRAMP TCW, as well as any changes to this content made in the SAP during planning.

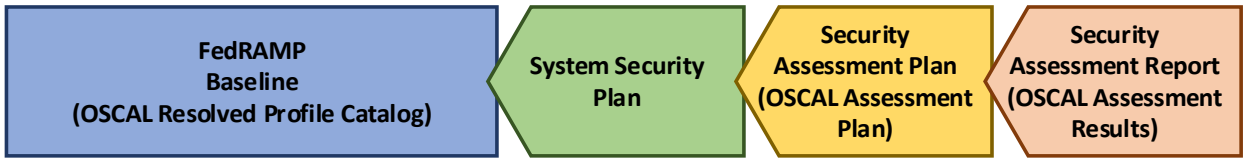
The only reason to include this content in the SAR is when there is a deviation from the SAP.

3.2.1. Resolved Profile Catalogs

The resolved profile catalog for each FedRAMP baseline is the result of pre-processing the profile and catalog to produce the resulting data. This can reduce 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. 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

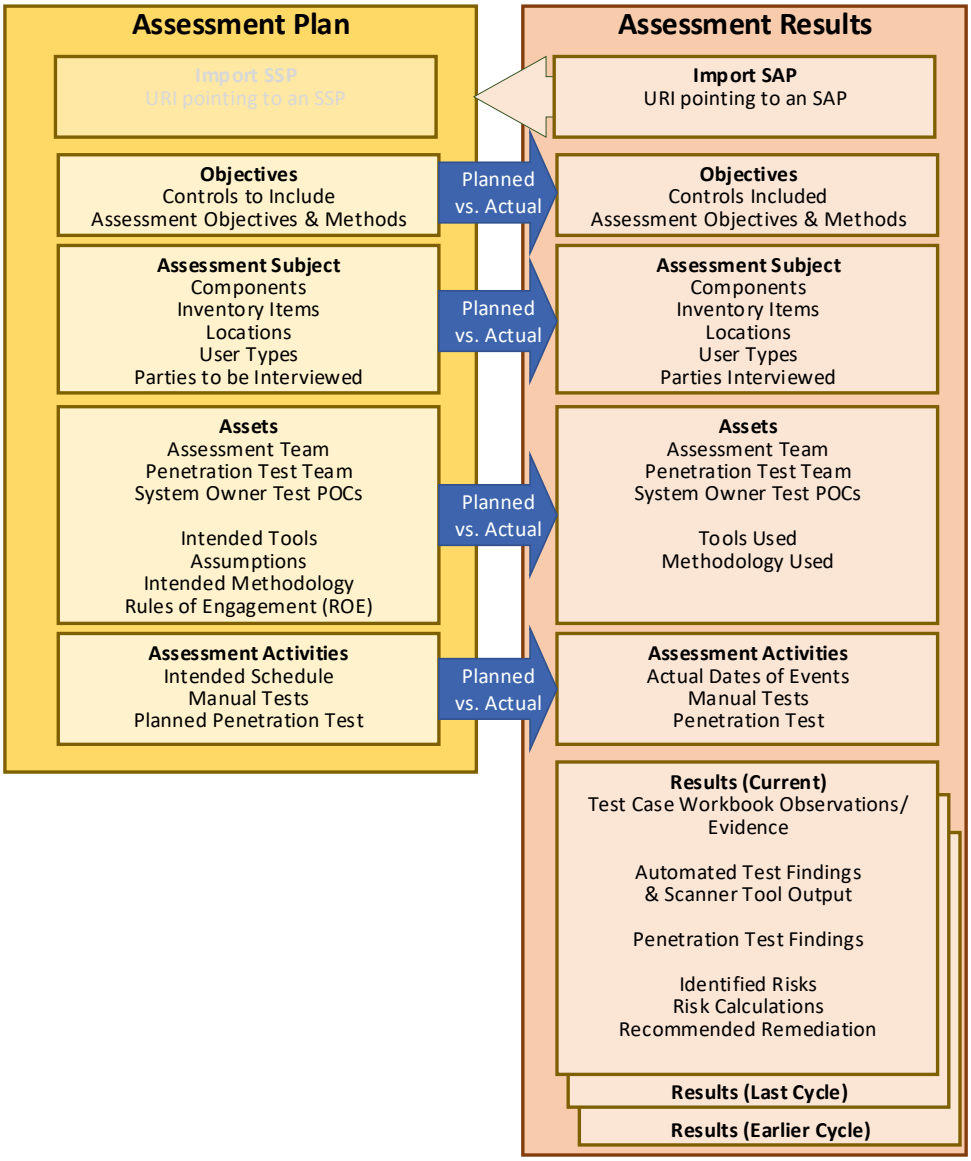
3.2.2. Assessment Deviations and SAP/SAR Syntax Overlap

The SAP plans the assessment. The SAR documents how the assessment was actually conducted in addition to reporting the results. For this reason all SAP syntax is included in the SAR syntax.

The operational concept is for an assessor to plan the assessment using the SAP syntax. When beginning the assessment, a tool can duplicate this content into the SAR as a starting point for the assessment team. As the assessment is performed, the assessment team updates this content to reflect what actually happened during the assessment.

For example, the SAP may say the assessment will start on June 1st and use five specific tools. The SAR may later reflect that the assessment actually started on June 3rd, and only used four specific tools. A tool would allow the assessor to adjust these details in the SAR.

Instead of an assessor manually summarizing assessment deviations, a tool can simply compare the SAP and SAR content, and report the differences automatically.

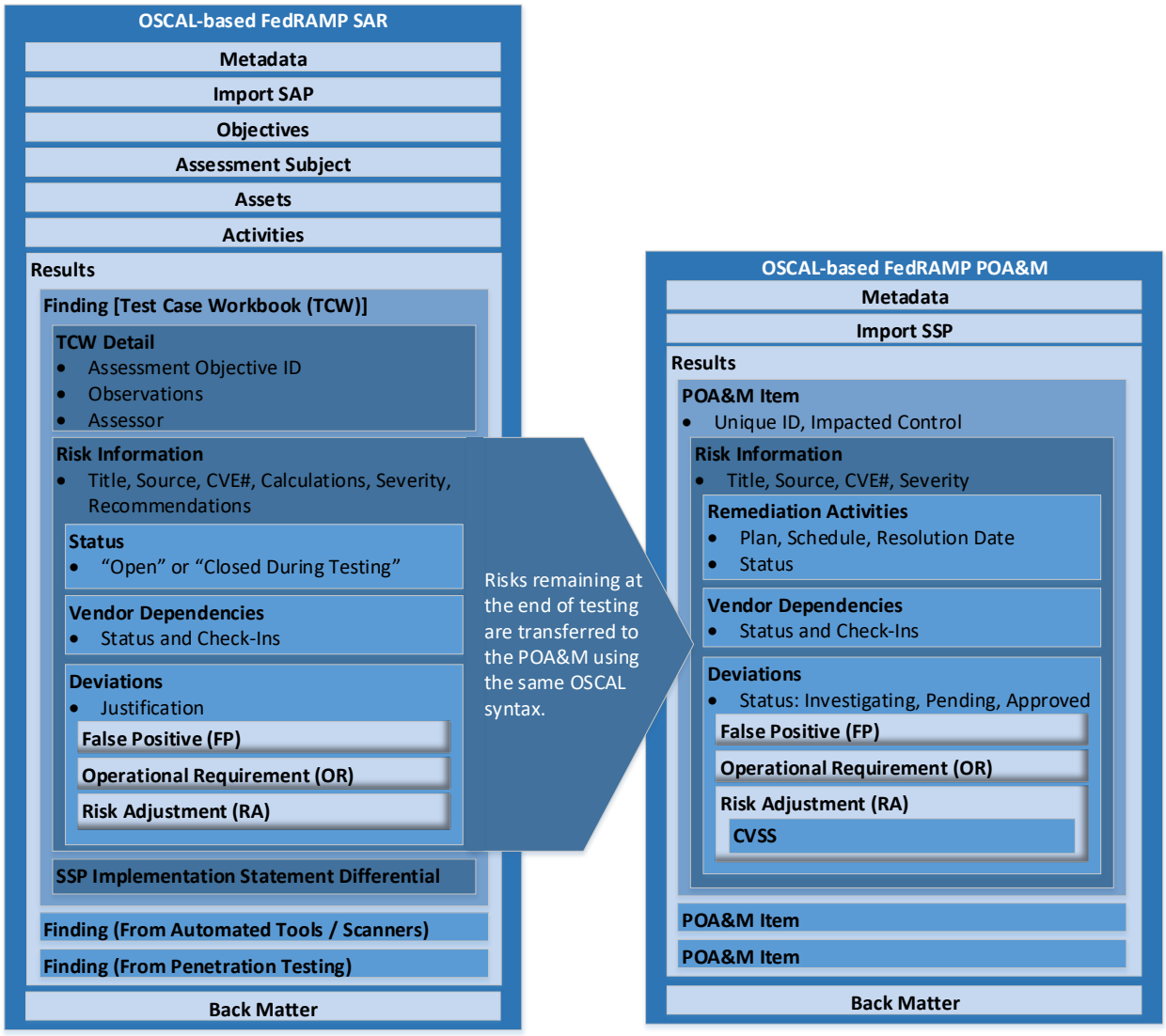


SAP/SAR tools can compare SAP and SAR content to report assessment deviations.

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

FedRAMP's requires residual risks from an initial or annual assessment to be reflected in the POA&M. The results portion of an OSCAL-based SAR uses the same syntax as the OSCAL based POA&M to enable easy transfer of residual risk information into the POA&M.

It is important to note that the content of a SAR is the assessor's responsibility, while the content of a POA&M is the system owner's responsibility; however, FedRAMP is aware some assessors will create or update a POA&M for the system owner. Regardless of who updates the POA&M, the common syntax enables easy transfer between a SAR tool and a POA&M tool.



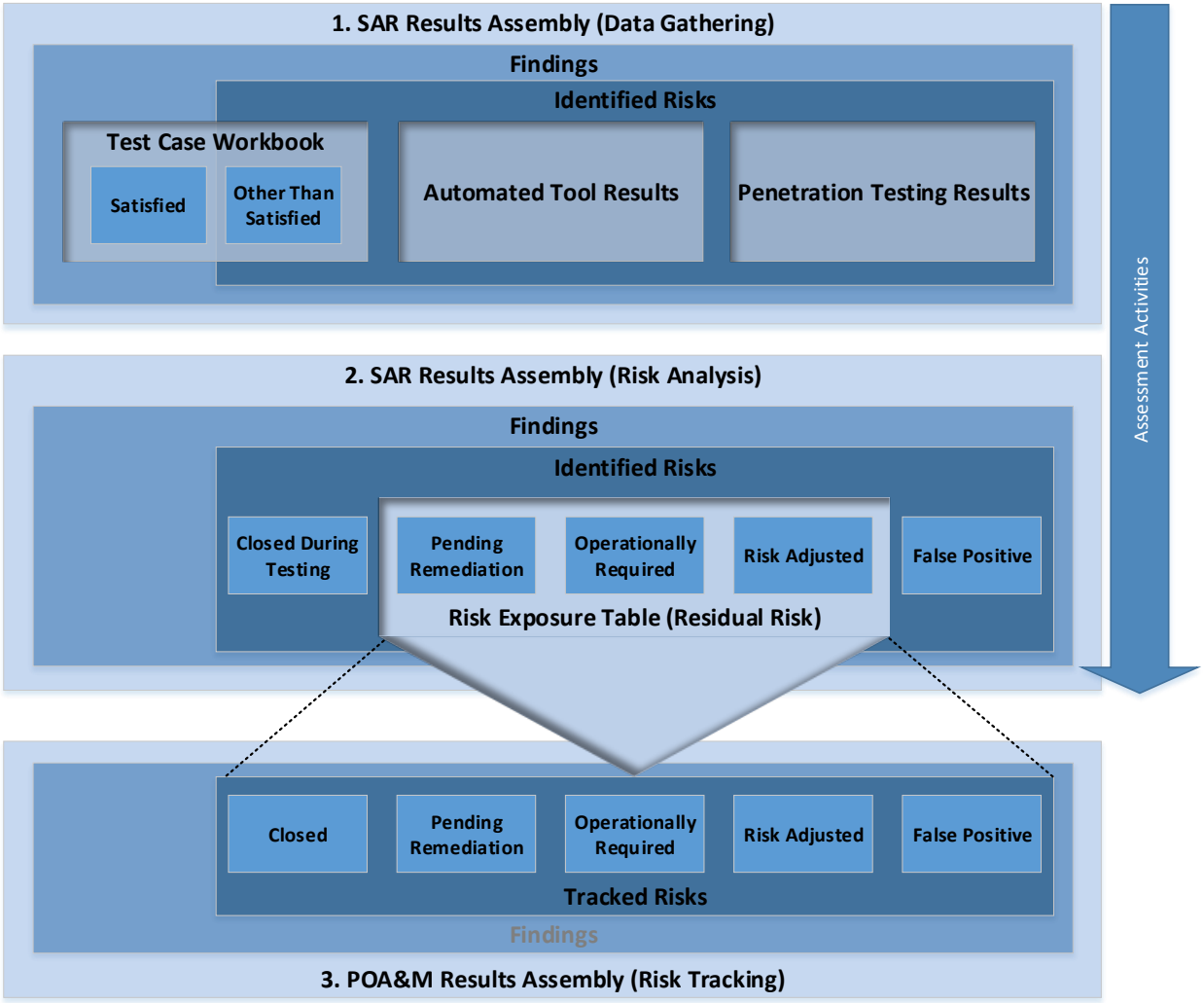
A SAR tool can transfer residual risks to a POA&M using the same OSCAL syntax.

A SAR tool should collect Test Case Workbook, Automated Tool Output, Manual Test Results, and Penetration Test Results as a series of individual Findings.

As these findings become risks, the SAR tool should allow the risk information to be added to the finding.

As risks are closed during testing, the SAR tool should allow the assessor to mark the status as closed. Likewise, as a risk is found to be a false positive or operationally required, the tool should allow the assessor to make these changes as well. The tool should also provide for risk adjustments, by preserving the initial risk information and adding mitigating factors and adjusted risk values.

Allowing for these adjustments, the Risk Exposure table is simply a "view" or presentation of the findings that have risks with an open status that have not been marked as a false positive. These are also the entries that are copied to the CSP's POA&M.

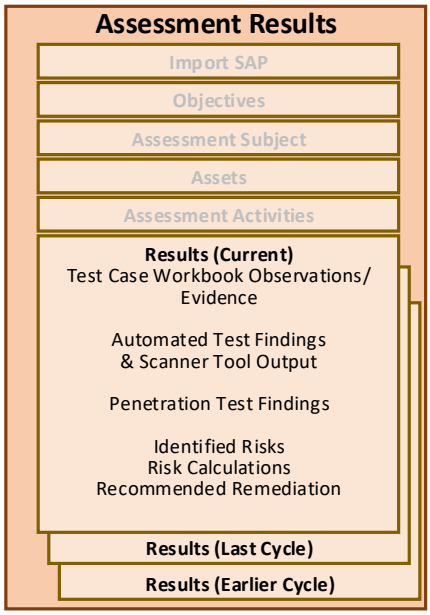


A SAR allows the assessor to update finding and risk information during the assessment.

3.2.4. Previous Assessment Results

The OSCAL assessment results model is designed to support both continuous assessment as well as snapshot in time assessments. Currently, FedRAMP assessments represent a snapshot in time. This means a single results assembly should be used for all of the current assessment findings.

Any findings from previous assessments may be included in the SAR by including each in its own results assembly. In this way, the assessor can include the "snapshot" of each previous assessment with the current assessment, eliminating the need to manually copy past findings into that portion of the TCW.



Each assessment cycle in its own results assembly

SAR Representation

```
<results uuid="d2b54365-1b4c-427c-a42d-5ad2932a0a73">
   <title>2020 Annual Assessment</title>
   <description></description>
   <start>2020-03-01T00:00:00Z</start>
   <end>2020-03-12T00:00:00Z</end>
   <!-- findings -->
</results>
<results uuid="fcaa8260-8254-49d3-9ca2-751bacd4b715">
   <title>2019 Annual Assessment</title>
   <description></description>
   <start>2019-03-01T00:00:00Z</start>
   <end>2019-03-12T00:00:00Z</end>
   <!-- findings -->
</results>
<results uuid="6608034d-aa14-4c82-b60d-57dc5aeeecee">
   <title>2018 Initial Assessment</title>
   <description></description>
   <start>2018-03-01T00:00:00Z</start>
   <end>2018-03-12T00:00:00Z</end>
   <!-- findings -->
</results>
```

XPath Queries

```
(SAR) Number of Assessments Represented:
  count(/*/results)

(SAR) Start Date of First Results Set:
  /*/results/start[1]

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

NOTE: Compare start dates of each result set to identify the newest.
```

3.3. OSCAL-based FedRAMP SAR Template

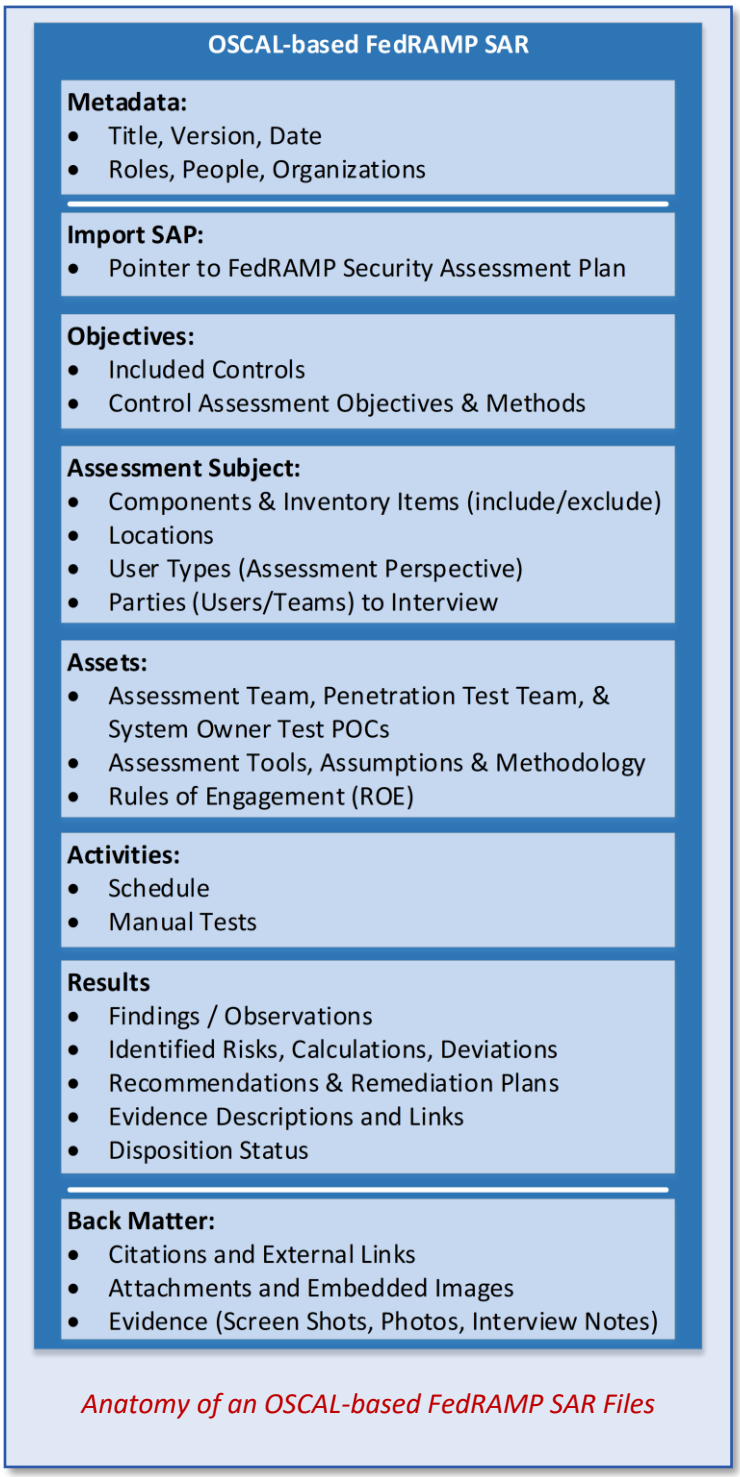
FedRAMP offers an OSCAL-based SAR shell file in both XML and JSON formats. This shell contains many of the FedRAMP required standards to help get you started. This document is intended to work in concert with that file. The OSCAL-based FedRAMP SAR Template is available in XML and JSON formats here:

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

3.4. OSCAL's Minimum File Requirements

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

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



Anatomy of an OSCAL-based FedRAMP SAR Files

The SAR is represented in OSCAL using the Assessment Results Model in the Assessment Results Layer.

In addition to the core OSCAL syntax, the following FedRAMP-specific implementation applies:

- **Import SAP**: Identifies the OSCAL-based SAP for this assessment. Several pieces of information about the assessment are cited from the SAP. The SAP imports the SSP, which provides several pieces of information about the system being assessed.
- **Objectives**: Identifies the controls to be included within the scope of this assessment, as well as the control objectives and assessment methods.
- **Assessment Subject**: Identifies the in-scope elements of the system, including locations, components, inventory items, and users.
- **Assets**: Identifies the assessor's assets used to perform the assessment, including the team, tool, and rules of engagement content.
- **Activities**: Describes the schedule, manual and automated tests, and other activities that may be explicitly be allowed or prohibited.
- **Results**: Describes the findings. A single syntax captures the Test Case Workbook content as well as the various SAR tables.

3.5. Importing the Security Assessment Plan

OSCAL is designed for traceability. Because of this, the assessment report is designed to be linked to the security assessment plan. Rather than duplicating content from the SSP and SAP, the SAR is intended to reference the SSP and SAP content itself.

Unavailable or Inaccurate OSCAL-based SSP Content

The SAR must import an OSCAL-based SAP, even if no OSCAL-based SSP exists.

FedRAMP enables an assessor to use the OSCAL SAP and SAR, when no OSCAL-based SSP exists, or where the assessor finds it to be inaccurate. The Guide to OSCAL-based FedRAMP Security Assessment Plans (SAP) describes when and how to represent missing or inaccurate SSP content.

SAR tools must search both the SSP (if any) and the SAP for any SSP-related references. If an ID in the SAR references content in both the SSP and the SAP, the tool should treat the SAP content as an update to the SSP content. See the Guide to OSCAL-based FedRAMP Security Assessment Plans (SAP) for more details.

Use the `import-ap` field to specify an existing OSCAL-based SAP. The href flag may include any valid uniform resource identifier (URI), including a relative path, absolute path, or URI fragment.

SAR Import Representation

```
   <import-ap href="../sap/FedRAMP-SAP-OSCAL-File.xml" />

- OR -

   <import-ap href="#attached-sap" />
```

XPath Queries

```
(SAR) URI to SSP:
  /*/import-ap/@href
```

If the value is a URI fragment, such as `#attached-sap`, the name to the right of the hashtag (#) is the ID value of a resource in the SAP file's `back-matter`. Refer to the *Guide to OSCAL-based FedRAMP Content*, *Section 2.6, Citations, Attachments and Embedded Content in OSCAL Files*, for guidance on handling.

SAR Back Matter Representation

```
<back-matter>
   <resource id="attached-sap">
      <title>[System Name] [FIPS-199 Level] SAP</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">sap</prop>
      <!-- Only one required. (XML or JSON, rlink or base64) -->
      <rlink media-type="application/xml" href="./CSP_System_SAP.xml" />
      <rlink media-type="application/json" href="./CSP_System_SAP.json" />
      <base64 media-type="application/xml" href="CSP_System_SAP.xml" />
      <base64 media-type="application/json" href="CSP_System_SAP.json" />
   </resource>
</back-matter>
```

Do Not Embed the SSP in the SAP

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

XPath Queries

```
(SAP) Referenced OSCAL-based SSP:
  /*/back-matter/resource[@id='ssp-ref']/rlink[@media-type=
  'application/xml']/@href
```

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

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

3.5.1. Ensuring Unique or Duplicate OSCAL IDs Where Appropriate

When a SAP field designates an ID for a `component`, `inventory-item`, `location`, or `user`, a SAP tool should look for the ID in both the appropriate section of the SSP and the SAP `local-definitions` (component, inventory-item, user) or `metadata` (location).

If the tool finds the ID in **either** the SSP or the SAP, the tool should use the content it finds, regardless of which file has the content.

If the tool finds ID in **both** the SSP and the SAP, the tool should consider the SSP to be original content and the SAP information to be a correction. In other words, SAP information should add to or override SSP information for the content identified by that ID.

If the tool does not find the ID in either location it should raise an error.

Tools Must Take Care with Duplicate IDs

In allowing for missing SSP content to be represented in the SAP, the potential exists for inadvertent duplication of IDs. The current state of OSCAL syntax validation tools will not catch this. Further, it may be necessary for a SAP tool to deliberately duplicate an SSP ID when correcting information.

3.6. Importing the FedRAMP Baseline

Once the content of the OSCAL-based SSP is accessible as a result of the actions in the previous section, the tool must then determine which FedRAMP baseline (profile) to open. Use the following query within the imported OSCAL-based SSP:

SSP XPath Queries

```
(SSP) Query the SSP for the Applicable Profile:
  /*/import-profile/@href
```

As with the `import-ssp` field in the previous section, this is any URI, including an absolute path, relative path, or URI fragment. If the value is a URI fragment, refer to the SSP's back-matter resource with that ID.

3.6.1. If No OSCAL-based SSP Exists (FedRAMP Baseline)

If no OSCAL-based SSP exists, as described in *Section* ***Error! Reference source not found.***, ***Error! Reference source not found.***, the resource with the `no-oscal-ssp` conformity tag must designate the applicable FedRAMP baseline using the FedRAMP OSCAL Extension `baseline-resource-id`, which contains the ID of another resource containing a link to the appropriate FedRAMP baseline.

SAP Representation

```
<import-ssp href="#ssp" />

<back-matter>
   <resource id="ssp-information">
      <title>System's Full Name</title>
      <prop name='conformity'
            ns='https://fedramp.gov/ns/oscal'>no-oscal-ssp-available</prop>
            ns="https://fedramp.gov/ns/oscal">FR00000000</prop>
      <prop name="baseline-resource-id" ns="https://fedramp.gov/ns/oscal">
                                          fedramp-moderate-baseline</prop>
   </resource>
</back-matter>
```

XPath Queries

```
(SAP) Path to Appropriate FedRAMP Baseline When No OSCAL-based SSP
  Exists:
  /*/back-matter/resource[@id=/*/back-matter/resource/prop
  [@name='conformity'] [@ns='https://fedramp.gov/ns/oscal']
  [string()='no-oscal-ssp']/../prop[@name='baseline-resource-id']
  [@ns='https://fedramp.gov/ns/oscal']]/rlink[@media-type=
  'application/xml']/@href

NOTE: Replace 'application/xml' with 'application/json' for JSON version of
  baseline.
```

The OSCAL-based FedRAMP SAP Template includes pre-loaded resources for the FedRAMP High, Moderate, and Low baselines. Their Resource IDs are `fedramp-high-baseline`, `fedramp-moderate-baseline` and `fedramp-low-baseline`.

4. SAR TEMPLATE TO OSCAL MAPPING

The OSCAL Assessment Results Model is used to represent the FedRAMP SAR. This model includes:

- Metadata and back-matter syntax, which is common to all OSCAL models;
- Assessment scope, subject, assets, and activities syntax, which is common to both the SAP and SAR; and
- Results syntax, which is common to the SAR and POA&M.

This guide assumes tool developers are already familiar with the *Guide to OSCAL-based FedRAMP Content* and the *Guide to OSCAL-based FedRAMP Security Assessment Plans (SAP)*.

Instead of duplicating content from those guides, this document refers to them and only add details that are unique to the SAR.

This section addresses the Test Case Workbook (TCW), Scanner Tool Results, Risks Identified during Penetration Testing, and the Risk Exposure Table (RET) first. These are addressed first because much of the individual SAR tables are generated from OSCAL-based this content.

As described in *Section 3, Working with OSCAL Files*, the SAP communicates the *intended* scope, subject, assets, and activities, and the SAR communicates the actual circumstances of the assessment. The same OSCAL syntax is used for this content in the SAP and SAR.

Assessment tools must enable assessors to duplicate the SAP content and modify it to reflect what actually happened during the assessment, including changes to the schedule, team, and tools used.

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

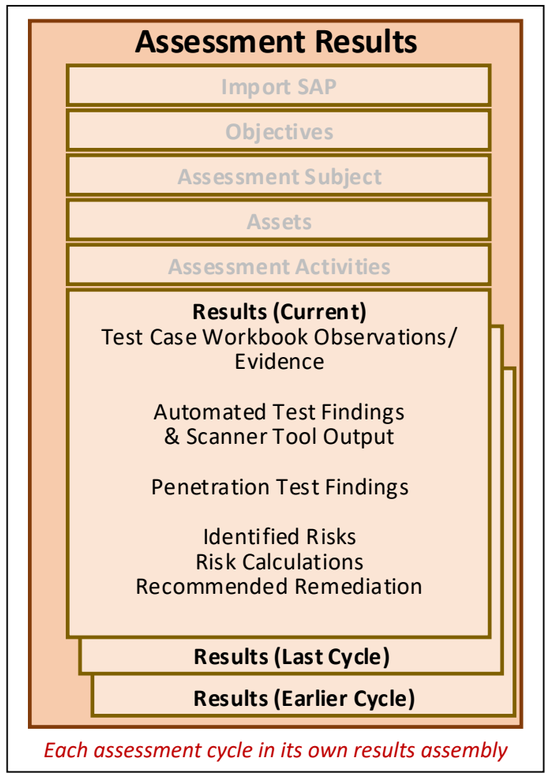
TOPIC	LOCATION
Title Page	*Guide to OSCAL-based FedRAMP Content, Section 4.1*
Prepared By/For	*Guide to OSCAL-based FedRAMP Content, Section 4.2 - 4.4*
Record of Template Changes	Not Applicable. Instead follow *Guide to OSCAL-based FedRAMP Content, Section 2.3.2, OSCAL Syntax Version*
Revision History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

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

- Table of Contents
- About This Document
- Who Should Use This Document
- How This Document is Organized
- SAR Section 3.3, Identification of Vulnerabilities
- SAR Section 3.4, Consideration of Threats
  - For convenience, the threats table can be found in the `threats` assembly in XML and JSON formats.
- SAR Section 3.5, Perform Risk Analysis
- SAR Section 3.6, Document Results

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

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



Each assessment cycle in its own results assembly

4.1. One Results Assembly for the Entire Assessment

All results from the current assessment must be in a single `results` assembly. Additional `results` assemblies are used for past assessment results. One `results` assembly for each past assessment results. This is covered in more detail in *Section 3.2.4, Previous Assessment Results*.

Tool developers must use the `start` field for each results assembly to determine the most recent set of results present in the SAR.

Representation

```
   <!-- assessment-activities -->
   <results uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
      <title>2020 Annual Assessment</title>
      <description><p>Brief assessment description.</p></description>
      <start>2020-03-01T00:00:00Z</start>
      <end>2020-03-12T00:00:00Z</end>
      <!-- TCW Findings -->
      <finding id="finding-1" />
      <finding id="finding-2" />
      <!-- Penetration Test Findings -->
      <finding id="finding-100" />
      <finding id="finding-101" />
      <!-- Automated Testing / Scanner Findings -->
      <finding id="finding-1000" />
      <finding id="finding-1001" />
   </results>

   <results uuid="301a0bd4-18aa-4c3e-a4a8-07f544d27266">
      <title>2019 Annual Assessment</title>
      <description><p>Brief assessment description.</p></description>
      <start>2019-02-01T00:00:00Z</start>
      <end>2019-02-12T00:00:00Z</end>
      <!-- findings -->
   </results>

   <results uuid="74803987-0313-4bbd-9347-edfaa8364f46">
      <title>2018 Initial Assessment</title>
      <description><p>Brief assessment description.</p></description>
      <start>2018-01-01T00:00:00Z</start>
      <end>2018-01-12T00:00:00Z</end>
      <!-- findings -->
   </results>
   <!-- back-matter -->
```

XPath Queries

```
(SAR) Quantity of assessment cycles present in file:
  count(/*/results)

(SAR) Start date/time of first assessment cycle results in file:
  /*/results/start[1]
```

NOTES:

- The `start` and `end` fields are dateTime-with-timezone. For FedRAMP initial and annual assessments, the time portion of this field may be all zeros as shown in the representation above.

4.2. Test Case Workbook: Assessment Objectives and Methods

There should be one `finding` assembly for each row in the Excel-based FedRAMP TCW. Tools must identify the appropriate FedRAMP baseline as described in *Section 3.6, Importing the FedRAMP Baseline*.

Every assessment objective identified in the FedRAMP baseline using the conformity tag, "`assessment-objective`" must have a `finding` entry in the `results` assembly. Use the following query to obtain the list of assessment objective IDs that must appear in the SAR.

Profile XPath Queries

```
(Baseline) List of FedRAMP Assessment Objectives (by ID):
  (/*/modify/alter/add/prop[@name='conformity']
  [@ns='https://fedramp.gov/ns/oscal'][string()='assessment-objective'] /../@id-ref)

(Baseline) List of Methods that must be used for the first objective:
  (/*/modify/alter/add/prop[@name='conformity']
  [@ns='https://fedramp.gov/ns/oscal'][string()='assessment-objective']/..)
  [1]/prop[@name='method']
```

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

For more information about generating the TCW assessment objectives, along with the examine, interview, and test instructions, see the *Guide to OSCAL-based Security Assessment Plans (SAP)*, *Section 5.3, Generating the "Test Case Workbook" List*.

NOTES:

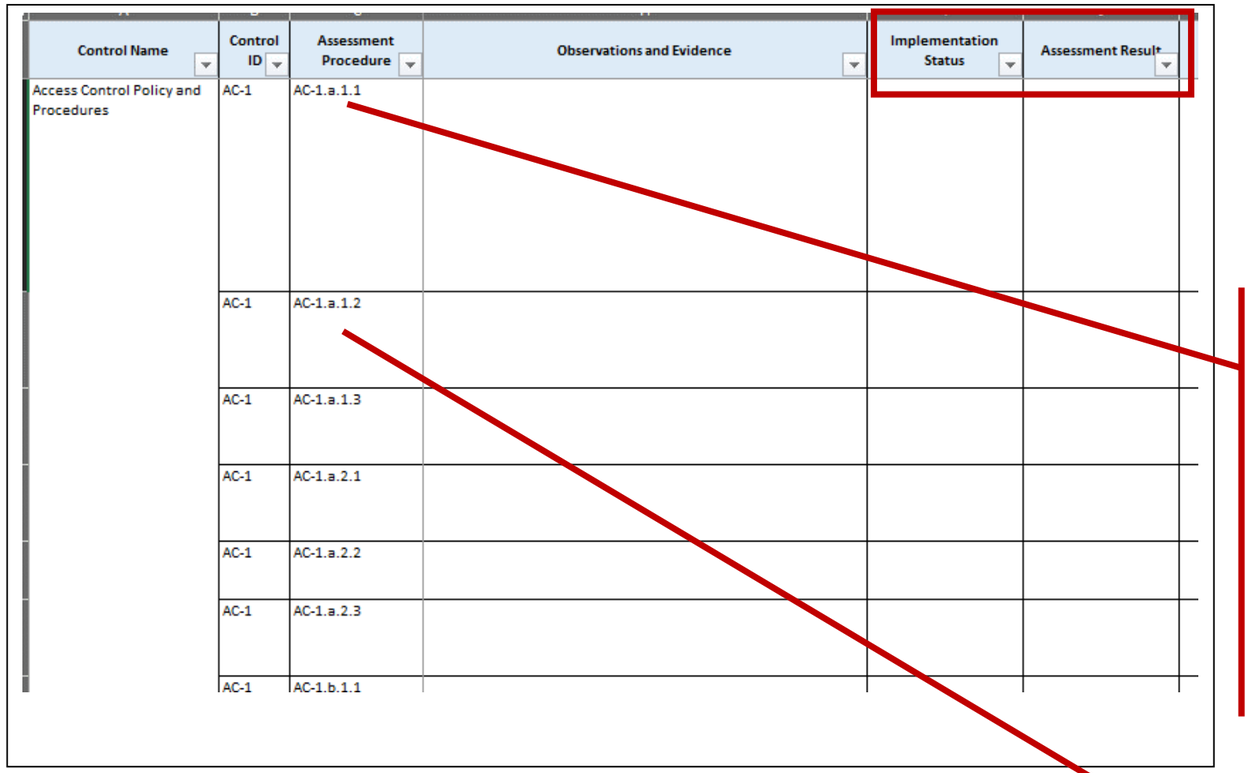
- .

Control Name	Control ID	Assessment Procedure	Assessment Objective	Examine	Interview	Test
Account Management | Automated Audit Actions	AC-2 (4)	AC-2(4).1	Determine if the information system: - automatically audits the following account actions: - creation - modification - enabling - disabling - removal		Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities	Automated mechanisms implementing account management functions
	AC-2 (4)	AC-2(4).2	Determine if the organization: - defines personnel or roles to be notified of the following account actions: - creation - modification - enabling - disabling - removal	Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; notifications/alerts of account creation, modification, enabling, disabling, and removal actions; information system audit records; other relevant documents or		
	AC-2 (4)	AC-2(4).3	Determine if the information system: - notifies organization-defined personnel or roles of the following account actions: - creation - modification - enabling - disabling - removal		Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities	Automated mechanisms implementing account management functions

HELPFUL HINTS

Use the appropriate FedRAMP resolved profile catalog, instead of the profile. This has the catalog content pre-merged, saving your tool the extra work of stepping through the profile to the catalog.

When processing an OSCAL-based FedRAMP baseline (profile or resolved-profile-catalog), each FedRAMP Test Case Workbook objective as a conformity tag of "`assessment-objective`".



Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

4.3. Test Case Workbook: Findings and Objective Status

There must be exactly one finding assembly for each assessment objective identified in the FedRAMP baseline. This is equivalent to having exactly one finding assembly for each row in the Excel-based FedRAMP TCW.

The objective-status assembly identifies which objective is being addressed by the assessor. It also holds the Implementation Status and Assessment Results fields.

Representation

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

   <finding uuid="30f81987-b773-4034-a54d-a75753cb5464">
      <title>TCW Objective</title>
      <description><p>May be empty.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <objective-status objective-id="ac-1.1_obj.1">
         <result system="https://fedramp.gov">satisfied</result>
         <implementation-status
             system="https://fedramp.gov">implemented</implementation-status>
      </objective-status>

      <!-- observation 1 -->
      <!-- observation 2 -->

      <!-- risk 1 -->
      <!-- risk 2 -->
      <!-- Assessor POCs for this objective -->
      <party-uuid>a56871e1-4c74-453c-9bab-c3367c6c0e3e</party-uuid>
      <party-uuid>3971c87b-c212-43b5-959d-2c9b39919401</party-uuid>
   </finding>

   <finding uuid="f05d2f06-1107-4ae6-befe-510d61e86536">
      <title>TCW Objective</title>
      <description><p>May be empty.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <objective-status objective-id="ac-1.1_obj.2">
         <result system="https://fedramp.gov">satisfied</result>
         <implementation-status
             system="https://fedramp.gov">implemented</implementation-status>
      </objective-status>

      <!-- observation 1 -->
      <!-- observation 2 -->

      <!-- risk 1 -->
      <!-- risk 2 -->
      <!-- Assessor POCs for this objective (Search SAP and SAR for these IDs)  -->
      <party-uuid>a56871e1-4c74-453c-9bab-c3367c6c0e3e</party-uuid>
      <party-uuid>3971c87b-c212-43b5-959d-2c9b39919401</party-uuid>
   </finding>

</results>
```

Accepted Values

- The `satisfaction` and `implementation-status` fields must each have the @system flag with a value of https://fedramp.gov
- The `satisfaction` field may only have one of the following values:
  - **`satisfied, other-than-satisfied`**
- The `implementation-status` field may only have one of the following values, which match the SSP accepted values:
  - **`implemented, partial, planned, alternative, not-applicable`**

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

The assessors who gathered the evidence are identified at the bottom of the finding assembly using `party-uuid` fields. The assessment team is defined as a `party` in the SAP `metadata`. If the assessor was not listed in the SAP, add a `party` to the SAR `metadata` for the assessor. In either case, a tool should list the UUID here, and should search both the SAP and SAR for the UUID when using this data.

See the next page for XPath Queries.

Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

Control Name	Control ID	Assessment Procedure	SSP Implementation Statement Differential	Assessor POC
Access Control Policy and Procedures	AC-1	AC-1.a.1.1		
	AC-1	AC-1.a.1.2		
	AC-1	AC-1.a.1.3		

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

The following assumes, the first `results` assembly contains the current assessment, as determined in *Section 4.1, One Results Assembly for the Entire Assessment*.

XPath Queries

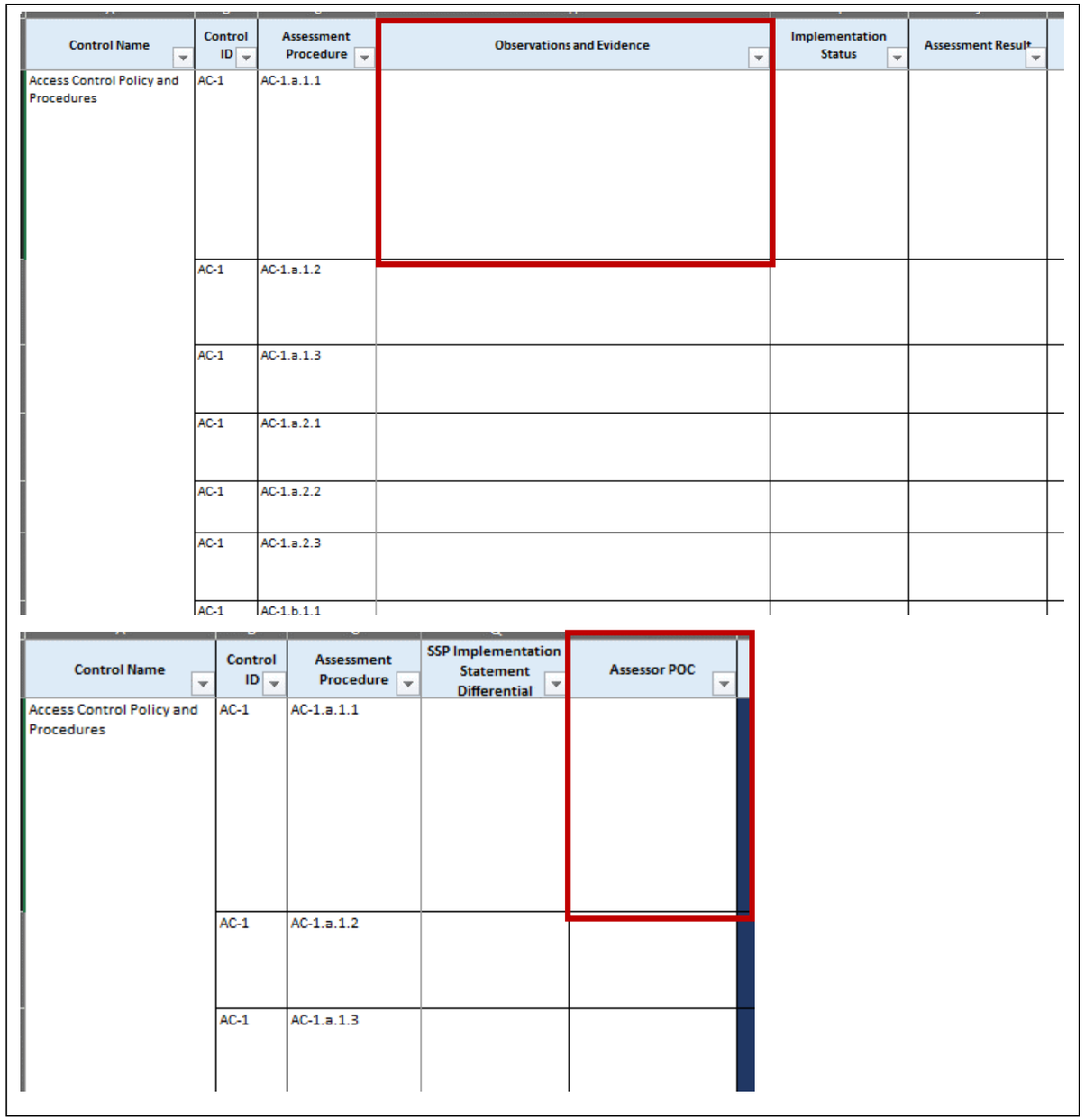
```
(SAR) Implementation Status:
  /*/results[1]/finding/objective-status [@objective-id='ac-1.a.1_obj.3']
  /implementation-status[@system='https://fedramp.gov']

(SAR) Assessment Result:
  /*/results[1]/finding/objective-status[@objective-id='ac-
  1.a.1_obj.3']/result[@system='https://fedramp.gov']

(SAR) Quantity of Assessor POC's cited for this objective (integer):
  count(/*/results[1]/finding/objective-status [@objective-id='ac-1.1 obj.1']
  /../party-id)

(SAR) Name of First Assessor POC cited for this objective:
  /*/metadata/party[@uuid=/*/results[1]/finding/objective-status
  [@objective-id='ac-1.1_obj.1']/../party-uuid][1]/person/person-name

NOTE: Replace 'person-name' with 'email' or 'phone' for contact information.
```



Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

Control Name	Control ID	Assessment Procedure	SSP Implementation Statement Differential	Assessor POC
Access Control Policy and Procedures	AC-1	AC-1.a.1.1		
	AC-1	AC-1.a.1.2		
	AC-1	AC-1.a.1.3		

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.4. Test Case Workbook: Observations and Evidence

The historic TCW spreadsheet only provided the assessor one cell for each Assessment Procedure to capture all observations and evidence. OSCAL enables observations to be broken down in to more granular detail, which further enables machine processing.

While each assessment procedure must have exactly one `finding` assembly, within the `finding` assembly there must be one or more `observation` assemblies. There should be at least one observation for each assessment method. For example, if an assessment procedure has both an EXAMINE method, there should be at least two observations, including at least one for TEST and at least one for EXAMINE. There may be more. Each `observation` should include the following:

GOAL	FIELD AND INFORMATION
Action: How was this assessed?	`observation-method (="EXAMINE", "INTERVIEW", "TEST")`
Categorize	`observation-type [="control-objective"]`
Actor: Who performed this action?	`assessor`
Subject: Who was Interviewed?	`subject-reference [type="party"]`
Subject: What was tested/inspected?	`subject-reference [type="component", "inventory-item", "resource" (Artifact)]`
How: What was used?	`reference [type="tool" or "method"]`
Evidence: What evidence supports this?	`relevant-evidence [type='observation']`

The following pages contains specific examples of Observations and Evidence.

Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

Accepted Values

For TWC, Observations and Evidence, the `observation-type` field must be set to:

- **`control-objective`**

The `observation-method` field may be set to one of the following:

- **`EXAMINE, INTERVIEW, or TEST`**

The `type` flag of the `subject-reference` field may be set to one of the following:

- **`component, inventory-item, location, party, user, or resource`**

The `type` flag of the `observation-source` field may be set to one of the following:

- **`tool, test-method, task, included-activity`**

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.4.1. TCW - Observations and Evidence: Examine

In the example below, the Access Control Policy was examined and found to be fully compliant. The `title` is discretionary.

The `description` describes the observation, and may include opinions

The `observation-method` is set to "`EXAMINE`" indicating this is in response to the EXAMINE activities prescribed for this objective.

The `observation-type` must be "`control-objective`" for all TCW Observations and Evidence content.

The `assessor` field points to an individual person identified as a `party` in the `metadata` assembly of either the SAP or SAR.

The `subject-reference` points to the policy that was reviewed. While OSCAL would allow the UUID to point to the policy attached to the SSP, FedRAMP requires assessors directly attach the artifacts and evidence to the SAR. Therefore, this should typically point to a `resource` in the SAR.

Finally, the `observation-source` points to the task in the SAP schedule, which describes the review of documentation.

Representation

```
<results uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <finding uuid="30f81987-b773-4034-a54d-a75753cb5464">
      <!-- title, description, date-time-stamp -->
      <objective-status objective-id="ac-1.a.1_obj.3">
         <satisfaction system="https://fedramp.gov">satisfied</satisfaction>
         <implementation-status
                  system="https://fedramp.gov">implemented</implementation-status>
      </objective-status>

      <observation uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab">
         <title>Examine AC Policy</title>
         <description>
            <p>[EXAMPLE]The AC policy existed, and had all the required elements.</p>
         </description>
         <observation-method>EXAMINE</observation-method>
         <observation-type>control-objective</observation-type>
         <assessor party-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
         <subject-reference uuid-ref="f32b7ab1-baf1-451a-b3a1-1dfdadbe8dc7"
                                                                  type="resource">
            <title>Reviewed Policy</title>
         </subject-reference>
         <observation-source type="task"
                                 uuid-ref="e1890486-a9f0-4388-b2bc-34fb6c623686" />
      </observation>

      <!-- observation: INTERVIEW -->
      <!-- risk -->
   </finding>
</results>
```

Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

Accepted Values

For TWC, Observations and Evidence, the `observation-type` field must be set to:

- **`control-objective`**

The `observation-method` field may be set to one of the following:

- **`EXAMINE, INTERVIEW, or TEST`**

The `type` flag of the `subject-reference` field may be set to one of the following:

- **`component, inventory-item, location, party, user, or resource`**

The `type` flag of the `observation-source` field may be set to one of the following:

- **`tool, test-method, task, included-activity`**

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.4.2. TCW - Observations and Evidence: Interview

In the example below, the Access Control Policy was examined and found to be fully compliant. The `title` is discretionary.

The `description` describes the observation, and may include opinions

The `observation-method` is set to "`INTERVIEW`" indicating this is in response to the INTERVIEW activities prescribed for this objective.

The `observation-type` must be "`control-objective`" for all TCW Observations and Evidence content.

The `assessor` field points to an individual person identified as a `party` in the `metadata` assembly of either the SAP or SAR.

The `subject-reference` points to the person interviewed, who may be listed in the SSP, SAP, or SAR.

The `observation-source` points to the task in the SAP schedule, which describes the interviewing of staff.

Finally, the `relevant-evidence` points to the attached interview notes as a URI fragment, and provides detail as to where the relevant statements are in the notes. While OSCAL will allow a relative external link in the `href` flag, FedRAMP requires each piece of evidence to be listed as a `resource` in the SAR back matter.

Representation

```
<results uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
   <!-- title, description, start, end -->
   <finding uuid="30f81987-b773-4034-a54d-a75753cb5464">
      <!-- title, description, date-time-stamp -->
      <objective-status objective-id="ac-1.a.1_obj.3">
         <satisfaction system="https://fedramp.gov">satisfied</satisfaction>
         <implementation-status
                  system="https://fedramp.gov">implemented</implementation-status>
      </objective-status>
      <!-- observation: EXAMINE -->

      <observation uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab">
         <title>AC Policy Interview</title>
         <description>
            <p>The person interviewed knew about the policy and where to find it.</p>
         </description>
         <observation-method>INTERVIEW</observation-method>
         <observation-type>control-objective</observation-type>
         <assessor party-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
         <subject-reference uuid-ref="5ff3d794-d2e8-48be-bf9c-95c2328271ce"
                                                                  type="party">
            <title>Interviewed Person</title>
         </subject-reference>
         <observation-source type="task"
                             uuid-ref="172d4ba2-3362-4e3b-9379-a65a50e399bf" />
         <relevant-evidence href="#65fb91b1-f7dc-46bf-8b99-bd98f1a5293d">
            <description>
               <p>Interview notes, page 4, item 2.</p>
            </description>
         </relevant-evidence>
      </observation>

      <!-- risk -->
   </finding>
</results>
```

Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

4.4.3. TCW - Observations and Evidence: Evidence and Artifacts

All artifacts reviewed and all evidence collected must be attached (by link or embedded Base64) as a resource in the back-matter. See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.6, Citations, Attachments, and Embedded Content in OSCAL Files* for more information.

Evidence must have the FedRAMP extension "`type`" with the value set to "`evidence`".

Reviewed Artifacts must have the FedRAMP extension "`type`" with the value set to "`artifact`".

Additional type fields may also be add with values such as plan, policy, or image. This adds clarity and can ensure specific tables are generated properly.

Artifacts may be cited from an `observation` as an `observation-source`.

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

A SAR tool could use either an `rlink` or `base64` field here, and may use both. If both are present, FedRAMP tools will give preference to the `base64` content. If an `rlink` is used, its href should have a relative path to ensure the path remains valid when the OSCAL content is delivered to FedRAMP.

Tools may include multiple `rlink` fields for the same resource. This may be useful if an assessor wanted to maintain an absolute link to the file's authoritative source location as well as a relative link suitable for delivery to FedRAMP.

Representation

```
   <!-- results -->
   <back-matter>
      <resource uuid="65fb91b1-f7dc-46bf-8b99-bd98f1a5293d">
         <title>[EXAMPLE]Interview Notes</title>
         <prop name="type" ns="https://fedramp.gov/ns/oscal">evidence</prop>
         <rlink media-type="application/msword" href="./interview-notes.docx"></rlink>
         <base64 media-type="application/msword"
                                    filename="interview-notes.docx">00000000</base64>
      </resource>

      <resource uuid="f32b7ab1-baf1-451a-b3a1-1dfdadbe8dc7">
         <title>[EXAMPLE]AC Policy</title>
         <prop name="type" ns="https://fedramp.gov/ns/oscal">artifact</prop>
         <prop name="type" ns="https://fedramp.gov/ns/oscal">policy</prop>
         <prop name="version">2.1</prop>
         <prop name="publication">2018-11-11T00:00:00Z</prop>
         <rlink media-type="application/pdf" href="./artifacts/AC_Policy.pdf"></rlink>
         <base64 media-type="application/pdf" filename="AC_Policy.pdf">00000000</base64>
      </resource>

      <resource uuid="53af7193-b25d-4ed2-a82f-5954d2d0df61">
         <title>[EXAMPLE]Screen Shot</title>
         <prop name="type" ns="https://fedramp.gov/ns/oscal">evidence</prop>
         <rlink media-type="image/jpeg" href="./evidence/screen-shot.jpg"></rlink>
         <base64 media-type="image/jepg" filename="screen-shot.jpg">00000000</base64>
      </resource>
   </back-matter>
```

Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

UUID References

OSCAL is designed around traceability, which means information is often referenced in its original location rather than duplicated into another file. As a result, it may be necessary to search the SSP, SAP, and/or SAR for a referenced UUID. To optimize tool searches, be aware of where to search for information based on a provided UUID.

For example, the `uuid-ref` value identified by `subject-reference` may be found in the SSP, SAP, or SAR, but mostly likely the SSP. For this reason it may make sense to always search the SSP first, SAP second, and SAR last.

Conversely, everything cited by `observation-source` must appear in the SAR, so only the SAR should be searched.

Other UUID references, such as party-uuid, will sometimes only be found in the SAR, sometimes the SAP or SAR, and sometimes possibly all three depending on the context.

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.4.4. TCW - Observations and Evidence: Queries

The following assumes, the first `results` assembly contains the current assessment, as determined in *Section 4.1, One Results Assembly for the Entire Assessment*.

XPath Queries

```
(SAR) Quantity of observations for this objective (integer):
  count(/*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation)

(SAR) The second observation for this objective:
  /*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[2]/description/node()

(SAR) SOURCE: Quantity of sources cited for the first observation in the first finding
  (integer):
  count(/*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[1]/observation-source)

(SAR) SOURCE: Type of source cited (first finding, first, observation, first source):
  /*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[1]/observation-source[1]/@type

(SAR) SOURCE: UUID of source cited (first finding, first, observation, first source):
  /*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[1]/observation-source[1]/@uuid-ref

(SAR) SUBJECT: Quantity of subjects cited, such as interviewed people, examined/tested
  system components, or reviewed artifacts (integer):
  count(/*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[1]/subject-reference)

(SAR) SUBJECT: Type of subject cited, such as interviewed people, examined/tested system
  components, or reviewed artifacts:
  /*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[1]/subject-reference[1]/@type

(SAR) SUBJECT: UUID of subject cited, such as interviewed people, examined/tested system
  components, or reviewed artifacts:
  /*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[1]/subject-reference[1]/@uuid-ref

(SAR) EVIDENCE: Quantity of evidence references for the second observation (integer):
  count(/*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[2]/relevant-evidence)

(SAR) EVIDENCE: Description of the first piece of evidence for the second observation:
  /*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[2]/relevant-evidence/description/node()

(SAR) EVIDENCE: The URI pointing to the evidence. For FedRAMP, the value should always
  be a URI fragment (starting with a '#' pointing to a back-matter resource:
  /*/results[1]/finding/objective-status[@objective-id='ac-1.a.1_obj.3']
  /../observation[2]/relevant-evidence/@href

(SAR) EVIDENCE: The back-matter resource containing the evidence (strip leading '#'):
  /*/back-matter/resource[@uuid='65fb91b1-f7dc-46bf-8b99-bd98f1a5293d']/rlink/@href

(SAR) EVIDENCE: The back-matter resource containing the evidence (strip leading '#'):
  /*/back-matter/resource[@uuid='65fb91b1-f7dc-46bf-8b99-bd98f1a5293d']/base64
```

Control Name	Control ID	Assessment Procedure	Observations and Evidence	Implementation Status	Assessment Result
Access Control Policy and Procedures	AC-1	AC-1.a.1.1			
	AC-1	AC-1.a.1.2			
	AC-1	AC-1.a.1.3			
	AC-1	AC-1.a.2.1			
	AC-1	AC-1.a.2.2			
	AC-1	AC-1.a.2.3			
	AC-1	AC-1.b.1.1			

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.4.5. Historic Test Case Workbook: Observations and Evidence

When converting historic Test Case Workbook content to OSCAL, many details broken down in a way that fits OSCAL. While refactoring old data to fit OSCAL is ideal and encouraged, it is not required for historic information.

There must still be one `finding` assembly for each row of the Test Case Workbook.

If no date or time is available for an individual row, use the `results` assembly's `start` field value.

Provide a single `observation` assembly in each `finding`, and put the entire TCW entry in the `description` field.

Finally, set the `observation-method` to "MIXED" and the `observation-type` to "`historic`".

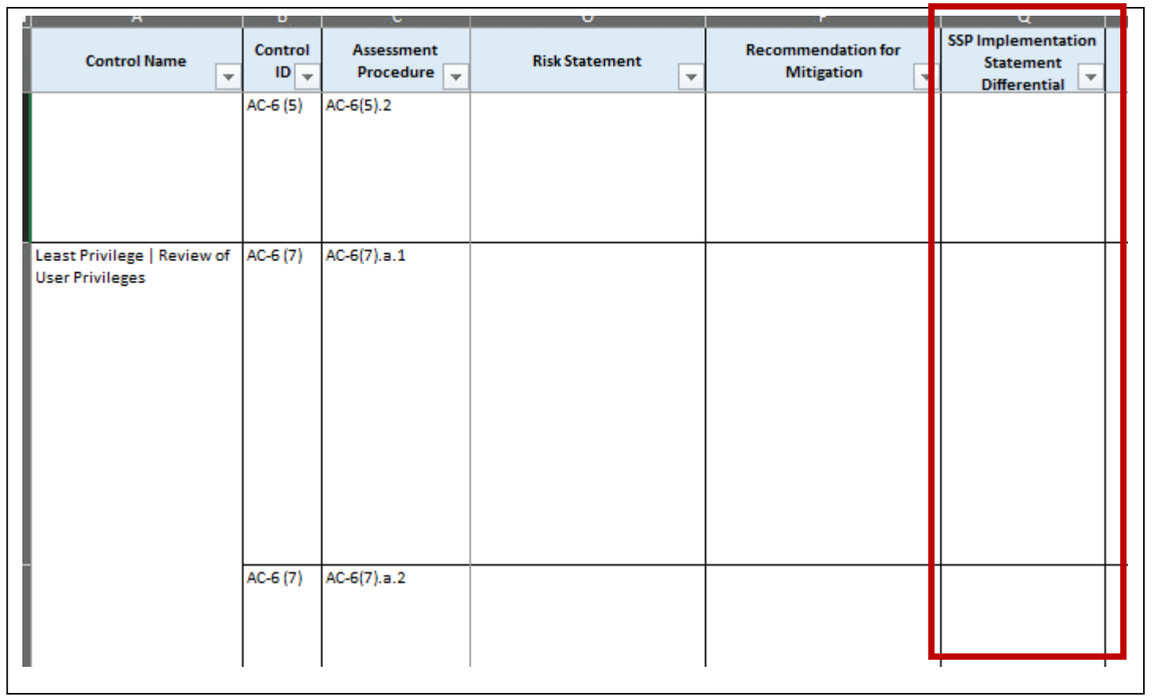
The Implementation Status, Assessment Results, and Assessor POC are handled the same as described in the above sections. The information is queried as described above as well.

Representation

```
<results uuid="d755e7fd-346d-40f0-b538-1b1da1aa5821">
   <title>Initial (2018) Assessment</title>
   <description/>
   <start>2018-03-01T00:00:00Z</start>
   <end>2018-03-12T00:00:00Z</end>
   <finding uuid="0cbd1819-3ea7-4f78-9ebc-92873eab4d6e">
      <title>AC-1.1.1.3</title>
      <description/>
      <date-time-stamp>2018-03-01T00:00:00Z</date-time-stamp>
      <objective-status objective-id="ac-1.1_obj.3">
         <result system="https://fedramp.gov">satisfied</result>
         <implementation-status
                  system="https://fedramp.gov">implemented</implementation-status>
      </objective-status>

      <observation uuid="1c23ddee-7001-4512-9de1-e062faa69c0a">
         <title>Observations and Evidence</title>
         <description>
            <p>Contents of the Observations and Evidence cell in the TCW.</p>
         </description>
         <observation-method>MIXED</observation-method>
         <observation-type>historic</observation-type>
         <assessor party-uuid="e934d8b5-13e5-4f77-b55e-871e6f2df2fe" />
      </observation>

   </finding>
   <!-- finding -->
   <!-- finding -->
</results>
```



Control Name	Control ID	Assessment Procedure	Risk Statement	Recommendation for Mitigation	SSP Implementation Statement Differential
	AC-6 (5)	AC-6(5).2			
Least Privilege | Review of User Privileges	AC-6 (7)	AC-6(7).a.1			
	AC-6 (7)	AC-6(7).a.2			

Accepted Values

For TWC, SSP Implementation Statement Differential, the `observation-type` field must be set to:

- **`ssp-statement-issue`**

The `observation-method` field must be set to:

- **`EXAMINE`**

If the `subject-reference` field is present, the `type` flag may be set to one of the following:

- **`component, inventory-item, location, party, user, or resource`**

The `type` flag of the `observation-source` field may be set to one of the following:

- **`tool, test-method, task, included-activity`**

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.5. Test Case Workbook: SSP Implementation Statement Differential

An SSP Implementation Statement Differential is simply another observation with an observation type of `implementation-statement`.

The `reference` field then identifies the deficient statement in the SSP. It must also have a type of `implementation-statement`.

If this was an issue where an inventory-item or component was not configured as described in the SSP, this observation could also include a `subject-reference` for any items that do not match the SSP.

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding uuid="33e43825-6fd7-49c6-a610-4c795954a167">
      <title>[EXAMPLE]Issue With AU-1 Statement</title>
      <description><p>[EXAMPLE]There is an issue with .</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>

      <implementation-statement-uuid>7924db51-e44d-4215-ad7e-3a5dda44a631
                                                    </implementation-statement-uuid>
      <observation uuid="3f955801-52ec-4846-aefe-7d27b79f1e2c">
         <title>[EXAMPLE]</title>
         <description>
            <p>SSP describes a procedure that does not exist in the repository.</p>
         </description>
         <observation-method>EXAMINE</observation-method>
         <observation-type>ssp-statement-issue</observation-type>
         <assessor party-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
         <observation-source type="task"
            uuid-ref="172d4ba2-3362-4e3b-9379-a65a50e399bf" />
         <relevant-evidence href="#53af7193-b25d-4ed2-a82f-5954d2d0df61">
            <description>
               <p>Screen shot showing list of procedures in the repository.</p>
            </description>
         </relevant-evidence>
      </observation>

   </finding>
</results>
```

The following assumes, the first `results` assembly contains the current assessment, as determined in *Section 4.1, One Results Assembly for the Entire Assessment*.

XPath Queries

```
(SAR) Quantity of SSP implementation statement differential issues cited in current
  assessment (integer):
  count(/*/results[1]/finding//observation/observation-type[string()='ssp-statement-
  issue'] )

(SAR) List of SSP implementation statement differential issues cited in current
  assessment (by SSP Statement UUID):
  /*/results[1]/finding//observation/observation-type[string()='ssp-statement-issue']
  /../../implementation-statement-uuid

(SAR) The description of the first deficiency:
  (/*/results[1]/finding//observation/observation-type[string()='ssp-statement-issue'])
  [1]/../description/node()
```

Control Name	Control ID	Assessment Procedure	Identified Risk	Likelihood Level	Impact Level	Risk Exposure Level	Risk Statement	Recommendation for Mitigation
Access Control Policy and Procedures	AC-1	AC-1.a.1.1						
	AC-1	AC-1.a.1.2						
	AC-1	AC-1.a.1.3						
	AC-1	AC-1.a.2.1						
	AC-1	AC-1.a.2.2						
	AC-1	AC-1.a.2.3						
	AC-1	AC-1.b.1.1						
	AC-1	AC-1.b.1.2						
	AC-1	AC-1.b.2.1						

Accepted Values

- The `risk-status` field should always be set to "`open`" when a risk content is first created.
- The `likelihood` and `impact` fields must each have one of the following values:
  - **low**
  - **moderate**
  - **high**
- The risk is calculated, consistent with Annual SAR Table 3-6, Risk Exposure Rating

Likelihood	Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

Table 3-6 – Risk Exposure Ratings

NOTE: The risk exposure can be found in the `risk-calculation` assembly available in XML and JSON formats, using the likelihood and impact values.

The `risk-statement` and `description` fields are *Markup multiline*, which enables the text to be formatted. See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.6. Test Case Workbook: Identified Risks

For any finding with a `result` value of '`other-than-satisfied`', there must be at least one `risk` assembly within the `finding` assembly. There must be one risk assembly for each identified risk. Risks may not be grouped. Instead use multiple assemblies.

The Identified risk content is described in the `description` field.

The Likelihood Level and Impact Level are each entered in a `prop` field. Even though OSCAL recognizes the `prop` names "`likelihood`" and "`impact`", the FedRAMP extension (`ns`) must be used because FedRAMP limits the accepted values.

The Risk Exposure Level must either be calculated by the SAR tool, or it may be found in the `risk-calculation` assembly available in XML and JSON formats, using the likelihood and impact values.

The Risk Statement is described in the `risk-statement` field.

Initially, the `risk-status` field should always be set to "`open`". If the risk is addressed by the CSP and verified by the assessor before assessment activities are complete, this may be set to "`closed`".

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding id="finding-1">
      <title>TCW Objective</title>
      <description><p>May be empty.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <!-- objective-status -->
      <!-- observation -->
      <!-- . -->
      <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
         <title>Risk Title</title>
         <description>
            <p>This is a description of the identified risk.</p>
         </description>

         <prop name="likelihood" class='initial'
                                 ns="https://fedramp.gov/ns/oscal">high</prop>
         <prop name="impact"     class='initial'
                                 ns="https://fedramp.gov/ns/oscal">moderate</prop>
         <!-- Risk Exposure Level must be calculated by the SAR Tool -->

         <risk-statement>
            <p>This is the Risk Statement.</p>
         </risk-statement>
         <!-- remediation (recommended) -->

         <risk-status>open</risk-status>
      </risk>
      <!-- Add additional risk assemblies as needed -->
      <!-- party-id -->
   </finding>
</results>
```

Control Name	Control ID	Assessment Procedure	Identified Risk	Likelihood Level	Impact Level	Risk Exposure Level	Risk Statement	Recommendation for Mitigation
Access Control Policy and Procedures	AC-1	AC-1.a.1.1						
	AC-1	AC-1.a.1.2						
	AC-1	AC-1.a.1.3						
	AC-1	AC-1.a.2.1						
	AC-1	AC-1.a.2.2						
	AC-1	AC-1.a.2.3						
	AC-1	AC-1.b.1.1						
	AC-1	AC-1.b.1.2						
	AC-1	AC-1.b.2.1						
	AC-1	AC-1.b.2.2						

Accepted Values

- The `type` flag on the `remediation` field must be set to:
  - **`recommendation`**
- The `type` flag on the `recommendation-origin` field :
  - **`party`**
  - **`tool`**

The `description` fields are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.6.1. Test Case Workbook: Recommendation for Mitigation

For the `risk` assembly, there must be a `remediation` assembly containing the assessors recommended mitigation. The `type` flag must be set to "`recommendation`".

There may be more than one `remediation` assembly. For example, a tool may provide a recommended remediation, and the assessor may want to add their own recommendation. This would result in two remediation assemblies.

Later, any SAR remediation recommendations may be transferred to the POA&M using this syntax, and the CSP will add yet another `remediation` assembly with their actual plan for remediation.

If the risk is closed during testing, there must be an additional `remediation`-assembly with a `type` value of "`final`".

The assessor's recommendation should appear in the `description` field.

The `recommendation-origin` field's type flag should be set to "`party`", and the `uuid-ref` should contain the UUID of either the assessment organization itself or the individual assessor making the recommendation.

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding id="finding-1">
      <title>TCW Objective</title>
      <description><p>May be empty.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <!-- objective-status -->
      <!-- observation -->
      <!-- . -->
      <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
         <!-- title, description, likelihood, impact, risk-statement -->

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

         <remediation uuid="9c3be116-9be2-4e34-b9ce-4f2b49975133"
                                                    type="recommendation">
            <title>Tool-Provided Recommendation</title>
            <description>
               <p>A description of the Recommendation for Remediation.</p>
            </description>
            <recommendation-origin type="tool"
                                   uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
         </remediation>


         <!-- risk-status -->
      </risk>
   </finding>
</results>
```

See the next page for XPath Queries.

Likelihood	Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

Table 3-6 – Risk Exposure Ratings

Risk Exposure Lookup

The risk exposure can be found in the `risk-calculation` assembly available in XML and JSON formats, using the likelihood and impact values.

The `risk-statement` and `description` fields are *Markup multiline*, which enables the text to be formatted. See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

The following assumes, the first `results` assembly contains the current assessment, as determined in *Section 4.1, One Results Assembly for the Entire Assessment*.

XPath Queries

```
(SAR) Quantity of TCW risks identified for all objectives (integer):
  count(/*/results[1]/finding[boolean(objective-status)]/risk)

NOTE: Does not include risks that are not associated with an objective, such as those
  identified by penetration testing or automated scanning. This also excludes any risks
  associated with SSP Implementation Statement Differentials.

(SAR) Quantity of TCW risks identified for all SSP Implementation Statement Issues
  (integer):
  count(/*/results[1]/finding[boolean(objective-status)]/risk)

(SAR) Description of first TCW:
  /*/results[1]/finding[boolean(objective-status)][1]/risk/description/node()

(SAR) Likelihood Level of first identified risk:
  /*/results[1]/finding[boolean(objective-status)][1]
  /risk/prop[@name='likelihood'][@ns='https://fedramp.gov/ns/oscal']

(SAR) Impact Level of first identified risk:
  /*/results[1]/finding[boolean(objective-status)][1]
  /risk/prop[@name='impact'][@ns='https://fedramp.gov/ns/oscal']

(FedRAMP Values) Risk Calculation based on Likelihood and Impact:
  /*/risk-calculation/value[@likelihood='moderate'][@impact='high']

(SAR) Risk Statement for first identified risk:
  /*/results[1]/finding[boolean(objective-status)][1]/risk/risk-statement/node()

(SAR) Risk Status:
  /*/results[1]/finding[boolean(objective-status)][1]/risk/risk-status
```

Control Name	Control ID	Assessment Procedure	Recommendation for Mitigation	SSP Implementation Statement Differential	Assessor POC		Prior Assessment Result	Prior Risk Exposure Lev
	AC-6 (5)	AC-6(5).2						
Least Privilege | Review of User Privileges	AC-6 (7)	AC-6(7).a.1						
	AC-6 (7)	AC-6(7).a.2						

Accepted Values

- The `likelihood` and `impact` fields must each have one of the following values:
  - **`low`**
  - **`moderate`**
  - **`high`**
- The risk is calculated, consistent with Annual SAR Table 3-6, Risk Exposure Rating

Likelihood	Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

Table 3-6 – Risk Exposure Ratings

NOTE: These can be looked up in the `risk-calculation` assembly available in XML and JSON formats.

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.7. Test Case Workbook: Previous Result and Risk Exposure Level

If the results assembly for previous assessments were included in the OSCAL-based SAR, only queries are required to see any past results. While the Excel-based Test Case Workbook only had space for the results immediately preceding the current assessment, a SAR tool could offer an assessor or reviewer more robust information by including all previous results or even trends.

The following queries only cover the equivalent information in the TCW. The query assumes the second results assembly contains the information from the assessment immediately preceding this one.

The *Prior Risk Exposure Level* must still be calculated using the likelihood and impact results for that assessment cycle.

XPath Queries

```
(SAR) Quantity of risks identified for this objective (integer):
  count(/*/results[2]/finding/objective-status[@objective-id='ac-1.1_obj.3'] /../risk)

(SAR) Prior Assessment Result:
  /*/results[2]/finding/objective-status[@objective-id='ac-1.1_obj.3']
  /result[@system='https://fedramp.gov']

(SAR) Prior Likelihood Level of first identified risk:
  /*/results[2]/finding/objective-status[@objective-id='ac-1.1_obj.3']
  /../risk[1]/prop[@name='likelihood'][@class='initial'][@ns='https://fedramp.gov/ns/oscal']

(SAR) Prior Impact Level of first identified risk:
  /*/results[2]/finding/objective-status[@objective-id='ac-1.1_obj.3']
  /../risk[1]/prop[@name='impact'][@class='initial'][@ns='https://fedramp.gov/ns/oscal']

(FedRAMP Values) Risk Calculation based on Prior Likelihood and Impact:
  /*/risk-calculation/value[@likelihood='moderate'][@impact='high']
```

There may be more than one likelihood prop field, including both initial and residual likelihood entries as well as entries that do not conform to FedRAMP's values.

There should always be one that has the `ns` flag set to "`https://fedramp.gov/ns/oscal`", and the `class` flag set to "`initial`". There may also be a FedRAMP likelihood with the `class` flag set to "`residual`". If residual risk is also present, both values should be displayed by a tool.

[Image intentionally left blank.]

4.8. Automated Tools

Automated scanning tool output is simply another finding; however, the `objective-status` is typically not present.

FedRAMP requires exactly one `finding` assembly for each unique vulnerability identified by the scanning tool. Within this `finding` assembly, there must be exactly one `observation` assembly.

The `date-time-stamp` field must be set to the automation tool's discovery timestamp.

Within the observation assembly, the `observation-method` field must be set to "`TEST`", and the `observation-type` field must be set to "`finding`".

The `uuid` flag of the `origin` field must identify the automated tool's UUID, and the `type` flag must be set to "`tool`". The scanning tool should have been previously defined in the SAP's `assets` assembly and copied to the SAR. If not, the scanning tool should be added to the SAR `assets` assembly as described in the *Guide to OSCAL-based Security Assessment Plans (SAP)*, *Section 4.14, SAP Test Plan: Testing Performed Using Automated Tools*.

The `href` flag in the `relevant-evidence` field must contain a URI fragment that points to the `resource` containing the raw tool output attached in the back-matter.

At the end of the `findings` assembly, the UUID for the tool operator must be listed as the `party-uuid` for the finding. There may be more than one.

Representation

```
   <results id="results-2">
      <!-- title, description, start, end -->
      <finding uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
         <title>Discovery Scan Results</title>
         <description><p>The results of the discovery scan.</p></description>
         <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
         <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
            <description>
               <p>Sample description.</p>
            </description>
            <observation-method>TEST</observation-method>
            <observation-type>finding</observation-type>

            <!-- subject-reference -->
            <!-- subject-reference -->

            <origin uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" type="tool" />

            <relevant-evidence href="#19a07333-4e87-46dc-abab-adad60e706b9">
               <description>
                  <p>Raw scanner tool output - discovery scan.</p>
               </description>
            </relevant-evidence>

         </observation>
         <party-uuid>f4568fda-c6d2-4640-adec-0012015af7d0</party-uuid>
         <party-uuid>e934d8b5-13e5-4f77-b55e-871e6f2df2fe</party-uuid>
      </finding>
   </results>
```

[Image intentionally left blank.]

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.8.1. Automated Tools: Discovery Scans

Any undocumented devices identified by the discovery scans must be added to the SAR's `local-definitions` assembly within the `assessment-subjects` assembly as either inventory-items or components, as described in the *Guide to OSCAL-based Security Assessment Plans (SAP)*, *Section 4.5, SAP IP Addresses Slated for Testing*.

This should include information such as IP address, host name, and OS, as well as any other details typically reported for an undocumented host. All component and inventory-item syntax from the SSP is available here. Each undocumented device should then be listed as an individual subject-reference.

If the assessor believes any of the undocumented devices represent a risk, the risk assembly may be added with the appropriate information; however, it is not automatically required for discovery scans..

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <title>Discovery Scan Results</title>
      <description><p>The results of the discovery scan.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
         <description>
            <p>Undocumented devices found on network.</p>
         </description>
         <observation-method>TEST</observation-method>
         <observation-type>finding</observation-type>
         <subject-reference type="inventory-item"
                            uuid-ref="f61f4408-2cb8-444a-a312-bc88412e7c61" />
         <subject-reference type="inventory-item"
                            uuid-ref="02075556-3660-4112-8982-02fc7d6fac00" />
         <subject-reference type="inventory-item"
                            uuid-ref="5efe2c07-9fdf-453a-8457-6471046082fb" />
         <subject-reference type="component"
                            uuid-ref="75b059f2-a9ba-40b1-a1e0-881196ca1ead" />

         <origin uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" type="tool" />

         <relevant-evidence href="#19a07333-4e87-46dc-abab-adad60e706b9">
            <description>
               <p>Raw scanner tool output - discovery scan.</p>
            </description>
         </relevant-evidence>

      </observation>
      <!-- risk -->
      <party-uuid>f4568fda-c6d2-4640-adec-0012015af7d0</party-uuid>
      <party-uuid>e934d8b5-13e5-4f77-b55e-871e6f2df2fe</party-uuid>
   </finding>
</results>
```

[Image intentionally left blank.]

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.8.2. Automated Tools: Identified Vulnerabilities

There must be one `finding` assembly for each unique vulnerability. All devices identified as having that unique vulnerability must be itemized with `subject-reference` fields in the `observations` assembly.

The individual components and inventory-items on which the scans are performed should already be marked as to whether authenticated scanning is possible.

All components and inventory-items found to have the vulnerability must be cited using their UUID in the subject-reference field. One subject-reference for each item.

The `uuid` flag of the `origin` field must be set to the tool's UUID, and the `type` flag must be set to "`tool`".

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding uuid="170dd310-1a92-4fcf-a12b-ebfa03d9e6d8">
      <title>[EXAMPLE]Infrastructure Scan Unique Vulnerability</title>
      <description><p>Example infrastructure scan finding.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <observation uuid="63fd3d97-26c9-4d4c-8d24-9fbc482b7f52">
         <description>
            <p>[EXAMPLE]Scanner Output.</p>
         </description>
         <observation-method>TEST</observation-method>
         <observation-type>finding</observation-type>
         <!-- subject-reference -->
         <!-- subject-reference -->

         <origin uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" type="tool" />

         <relevant-evidence href="#171b44a2-9b52-4c46-b912-54bd274b2761">
            <description>
               <p>Raw scanner tool output - Infrastructure and OS Scan.</p>
            </description>
         </relevant-evidence>
      </observation>
      <!-- risk - Exactly one. See next page. -->
</results>
```

See next page for risk assembly

[Image intentionally left blank.]

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

The `risk` assembly uses `risk-metric` fields to capture relevant tool output details. The `system` flag allows `risk-metric` fields from different tools and different security frameworks to co-exist in the same file.

FedRAMP required risk-metric fields, such as likelihood and impact, have a system flag with a value of "https://fedramp.gov". FedRAMP required risk metrics must also have the class flag set to either "initial" or "residual". There must always be an intimal risk metric. If adjusted, there may be a residual risk metric as well.

The `uuid` flag of the `origin` field must be set to the tool's UUID, and the `type` flag must be set to "`tool`".

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding uuid="170dd310-1a92-4fcf-a12b-ebfa03d9e6d8">
      <title>[EXAMPLE]Infrastructure Scan Unique Vulnerability</title>
      <description><p>Example infrastructure scan finding.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <!-- observation: impacted hosts, tool used, link to raw scans -->
      <risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
         <title>Vulnerability Title</title>
         <description>
            <p>This is a description of the vulnerability provided by the tool.</p>
         </description>

         <risk-metric name="vulnerability-id"
                                 system="scanner-name">VulID-001</risk-metric>
         <risk-metric name="plugin-id"
                                 system="scanner-name">Plugin-ID</risk-metric>
         <risk-metric name="iavm-severity"
                                 system="scanner-name"></risk-metric>
         <risk-metric name="AV"
                                 system="CVSSv3.1">network</risk-metric>

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

         <risk-metric name="impact"     class="initial"
                           system="scanner-name">tool-provided-severity</risk-metric>
         <risk-metric name="impact"     class='initial'
                           system="https://fedramp.gov">high</risk-metric>
         <risk-metric name="likelihood" class='initial'
                           system="https://fedramp.gov">high</risk-metric>
         <risk-metric name="priority"
                           system="https://fedramp.gov">1</risk-metric>

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

         <!-- remediation: recommendation -->

         <risk-status>open</risk-status>
      </risk>
   </results>
```

For information about the remediation assembly, see *Section 4.6.1, Test Case Workbook: Recommendation for Mitigation*.

Likelihood	Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

Table 3-6 – Risk Exposure Ratings

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.9. Penetration Testing: Identified Risks

For any finding with a `satisfaction` value of '`other-than-satisfied`', there must be at least one `risk` assembly within the `finding` assembly. There may be more than one `risk` assembly.

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding id="finding-1">
      <title>TCW Objective</title>
      <description><p>May be empty.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <!-- objective-status -->
      <!-- observation -->
      <!-- observation -->
      <!-- . -->
      <risk id="risk-1">
         <title>Risk Title</title>
         <description>
            <p>This is a description of the identified risk.</p>
         </description>

         <prop name="likelihood" class='initial'
                                 ns="https://fedramp.gov/ns/oscal">moderate</prop>
         <prop name="impact"     class='initial'
                                 ns="https://fedramp.gov/ns/oscal">moderate</prop>
         <!-- SAR Tool Calculates Risk -->
         <risk-statement>
            <p>This is a statement about the identified risk.</p>
         </risk-statement>

         <remediation id="rem-1" type="recommendation">
            <title></title>
            <description>
               <p>A description of the recommended remediation.</p>
            </description>
            <id-ref id="assessor" type="party" />
         </remediation>

         <risk-status>open</risk-status>
      </risk>
      <!-- Add additional risk assemblies as needed -->
      <!-- party-id -->
   </finding>
</results>
```

5. GENERATED CONTENT

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

- **Assessment Summary**
- **System Overview (Categorization, Description, and Purpose)**
- **Scope**
- **Assessment Methodology**
- **Perform Tests**
- **Assessment Deviations**
- **Risk Exposure Table**
- **Risks Corrected During Testing**
- **Risks with Mitigating Factors**
- **Risks Remaining Due to Operational Requirements**
- **Risks Known for Interconnected Systems**
- **Scan Results (Infrastructure, Database, Web Application, Other, and Unauthenticated)**
    - **Inventory of Items Scanned**
    - **False Positive Report**
- **Assessment Results:**
    - **Table F-1: Summary of System Security Risks**
    - **Table F-2: Final Summary of System Security Risks**
    - **Table F-3: Open POA&Ms**
    - **Table F-4: Summary of Existing POA&Ms**
    - **Table F-5: Summary of Vulnerabilities Carried Forward**
    - **Table F-6: Summary of Unauthenticated Scans**
- **Manual Test Results**
- **Test Case Workbook's System Tab**
- **Test Case Workbook's CtrlSummary Tab**

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.

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

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

APPENDICIES

APPENDIX A. CVSS SCORING

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

The FedRAMP OSCAL Registry includes a tab with the specific `name` and `class` flag values to use for CVSS versions 2, 3 and 3.1. An OSCAL file may use either the all upper-case abbreviation, or the all lower-case name for each CVSS metric.

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding id="finding-1">
      <title>TCW Objective</title>
      <description><p>May be empty.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <!-- objective-status -->
      <!-- observation -->
      <risk id="risk-3-1">
         <title>Vulnerability Title</title>
         <description />

         <!-- CVSS Metrics using V3.1 abbreviations -->
         <prop name="AV" class="CVSSv3.1"
               ns="https://fedramp.gov/ns/oscal">network</prop>

         <prop name="AC" class="CVSSv3.1"
               ns="https://fedramp.gov/ns/oscal">high</prop>

         <prop name="PR" class="CVSSv3.1"
               ns="https://fedramp.gov/ns/oscal">low</prop>

         <!-- CVSS Metrics using V3.1 names -->
         <prop name="access-vector"       class="CVSSv3.1"
               ns="https://fedramp.gov/ns/oscal">network</prop>

         <prop name="access-complexity"   class="CVSSv3.1"
               ns="https://fedramp.gov/ns/oscal">high</prop>

         <prop name="privileges-required" class="CVSSv3.1"
               ns="https://fedramp.gov/ns/oscal">low</prop>

      <!-- observation -->
      <!-- risk-status -->
      </risk>
      <!-- party-id -->
   </finding>
```

At this time, CVSS metrics in OSCAL has not been formally coordinated with NIST nor the Forum of Incident Response and Security Teams (FIRST), and must be treated as a FedRAMP Extension.