FedRAMP™

Guide to OSCAL-Based FedRAMP® Security Assessment Reports (SAR) – Rev5

User Implementation Guide

Fedramp2.0.0-oscal1.0.x

June 30, 2023

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 SAR 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 Security Assessment Report (SAR) content.

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

1.2. Related Documents

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

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.

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 National Institute of Standards and Technology (NIST) in the creation of OSCAL syntax.

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

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

2. FedRAMP Extensions and Allowed Values

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

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

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

As a result, FedRAMP-compliant OSCAL files are a combination of the core OSCAL syntax and extensions defined by FedRAMP. The *Guide to OSCAL-Based FedRAMP Content* describes the concepts behind FedRAMP extensions and allowed values. The extensions related to the Security Assessment Plan (SAP) are cited in this document in context of their use.

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

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

Revised FedRAMP Registry Approach

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

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

3. Working with OSCAL Files

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

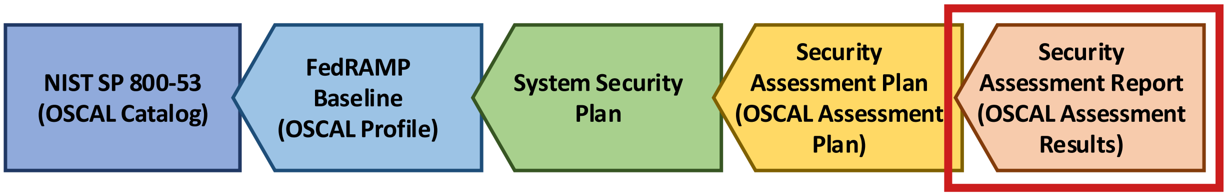
3.1. XML and JSON Formats

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.

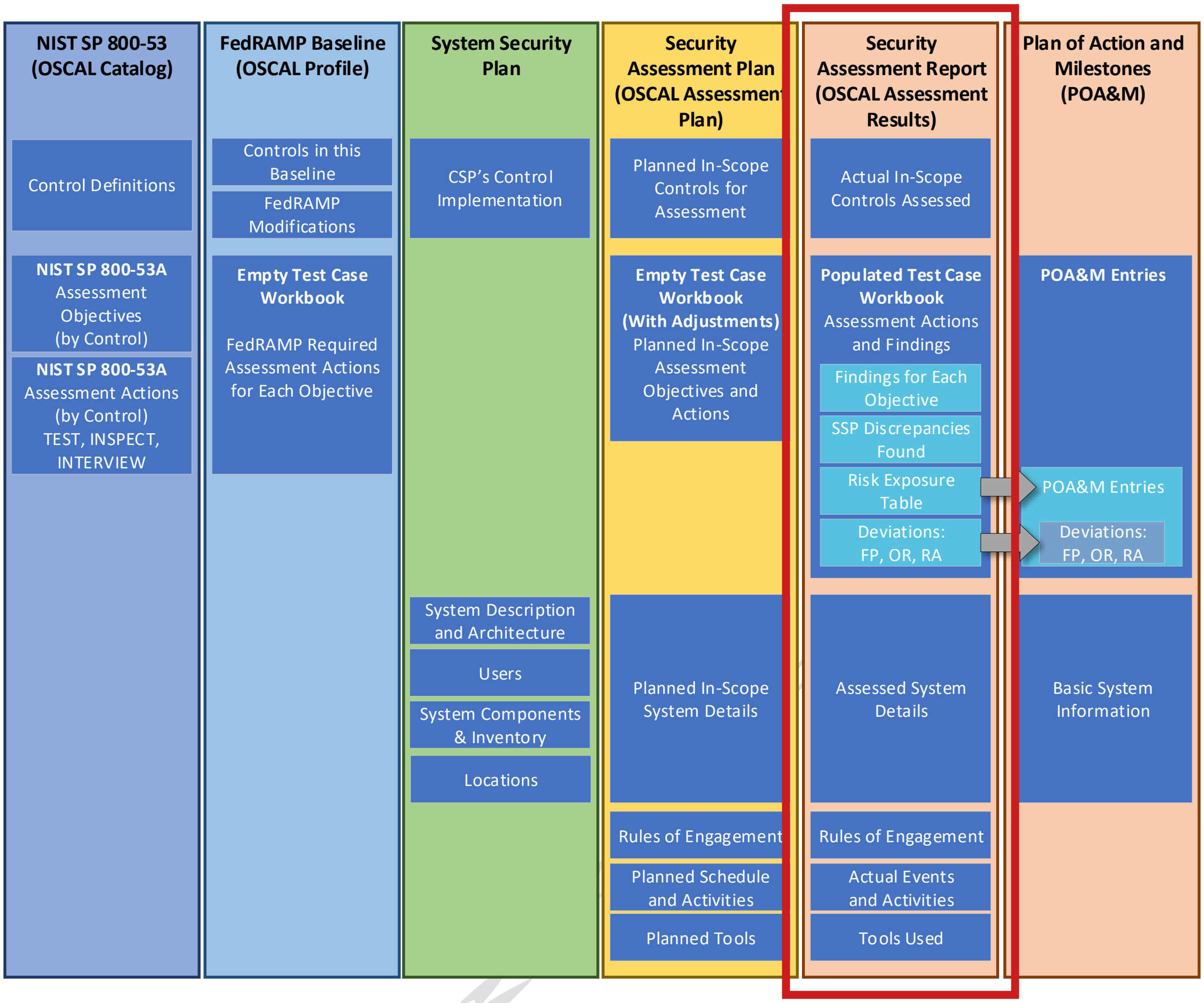
3.2. SAR File Concepts

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.


NIST SP 800-53 (OSCAL Catalog)
FedRAMP Baseline (OSCAL Profile)
System Security Plan
Security Assessment Plan (OSCAL Assessment Plan)
Security Assessment Report (OSCAL Assessment Results)

Each OSCAL file imports information from the one to the left

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


NIST SP 800-53 (OSCAL Catalog)
Control Definitions
NIST SP 800-53A Assessment Objectives (by Control)
NIST SP 800-53A Assessment Actions (by Control) TEST, INSPECT, INTERVIEW
FedRAMP Baseline (OSCAL Profile)
Controls in this Baseline
FedRAMP Modifications
Empty Test Case Workbook
FedRAMP Required Assessment Actions for Each Objective
System Security Plan
CSP's Control Implementation
System Description and Architecture
Users
System Components & Inventory
Locations
Security Assessment Plan (OSCAL Assessment Plan)
Planned In-Scope Controls for Assessment
Empty Test Case Workbook (With Adjustments) Planned In-Scope Assessment Objectives and Actions
Planned In-Scope System Details
Rules of Engagement
Planned Schedule and Activities
Planned Tools
Security Assessment Report (OSCAL Assessment Results)
Actual In-Scope Controls Assessed
Populated Test Case Workbook Assessment Actions and Findings
Findings for Each Objective
SSP Discrepancies Found
Risk Exposure Table
Deviations: FP, OR, RA
Assessed System Details
Rules of Engagement
Actual Events and Activities
Tools Used
Plan of Action and Milestones (POA&M)
POA&M Entries
POA&M Entries
Deviations: FP, OR, RA
Basic System Information

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.

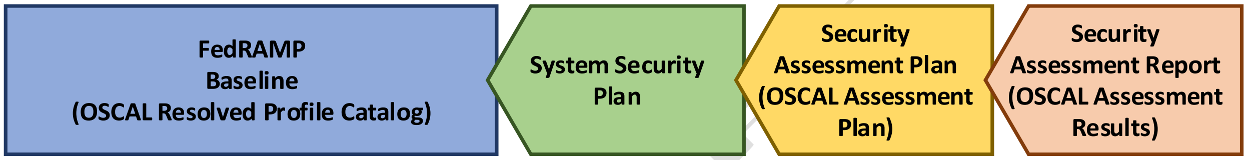
The only reason to include this content in the SAR is when there is a deviation from the SAP.

3.2.1. Resolved Profile Catalogs

The resolved profile catalog for each FedRAMP baseline is 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 for the separate profile and catalog handling later in their product roadmap.


FedRAMP Baseline (OSCAL Resolved Profile Catalog)
System Security Plan
Security Assessment Plan (OSCAL Assessment Plan)
Security Assessment Report (OSCAL Assessment Results)

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*.

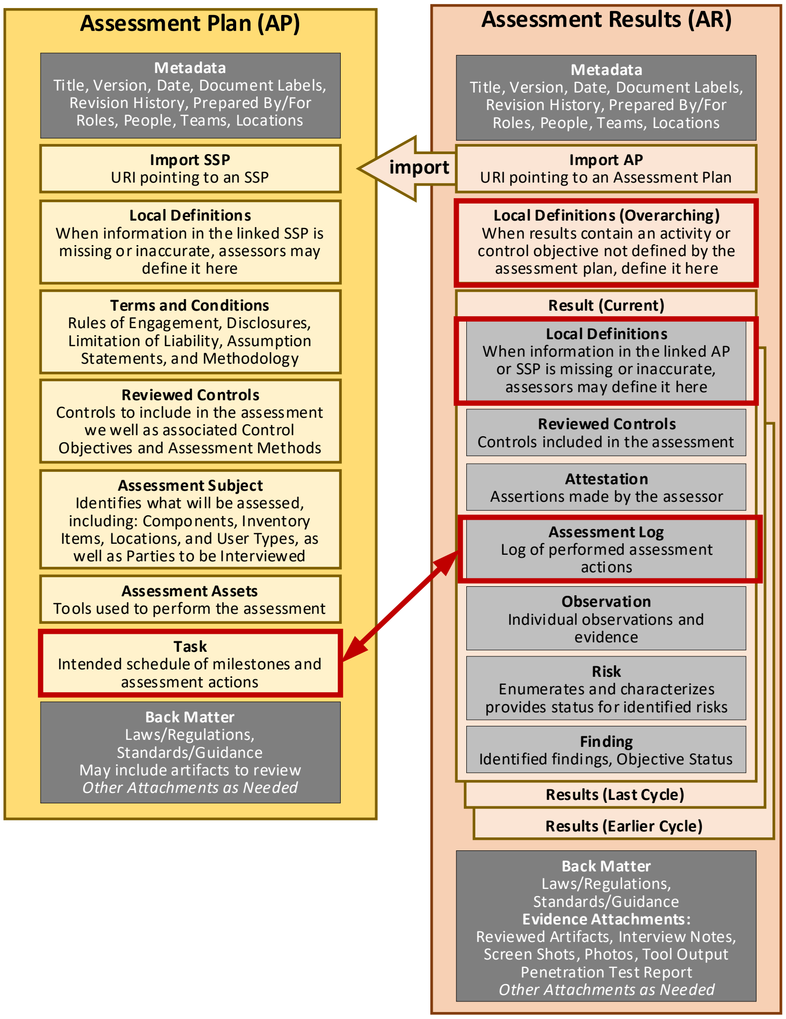
3.2.2. Assessment Deviations and SAP/SAR Syntax Overlap

The SAP represents the assessment intentions before it starts and should not be modified once the assessment starts. The SAR represents what actually happened during the assessment, in addition to reporting the results.

The SAR reference SAP content when those references are accurate and defines content locally when the assessment details deviate from the SAP. Similarly, the SAR's assessment log captures the actual timing of events and can be linked to the SAP's defined tasks (schedule).

FedRAMP's requirement to report assessment deviations can be very straightforward if the above approach is supported by tools.

For schedule deviations, a SAR's tools can simply compare the SAR assessment log to the SAP tasks and report differences.


Assessment Plan (AP)
Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations
Import SSP
URI pointing to an SSP
Local Definitions
When information in the linked SSP is missing or inaccurate, assessors may define it here
Terms and Conditions
Rules of Engagement, Disclosures, Limitation of Liability, Assumption Statements, and Methodology
Reviewed Controls
Controls to include in the assessment we well as associated Control Objectives and Assessment Methods
Assessment Subject
Identifies what will be assessed, including: Components, Inventory Items, Locations, and User Types, as well as Parties to be Interviewed
Assessment Assets
Tools used to perform the assessment
Task
Intended schedule of milestones and assessment actions
Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed
import
Assessment Results (AR)
Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations
Import AP
URI pointing to an Assessment Plan
Local Definitions (Overarching)
When results contain an activity or control objective not defined by the assessment plan, define it here
Result (Current)
Local Definitions
When information in the linked AP or SSP is missing or inaccurate, assessors may define it here
Reviewed Controls
Controls included in the assessment
Attestation
Assertions made by the assessor
Assessment Log
Log of performed assessment actions
Observation
Individual observations and evidence
Risk
Enumerates and characterizes provides status for identified risks
Finding
Identified findings, Objective Status
Results (Last Cycle)
Results (Earlier Cycle)
Back Matter
Laws/Regulations, Standards/Guidance
Evidence Attachments:
Reviewed Artifacts, Interview Notes, Screen Shots, Photos, Tool Output
Penetration Test Report
Other Attachments as Needed

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

Any other changes are essentially summarized in the SAR's local definitions. The overarching local definitions captures changes to defined activities or control objectives. The "Result" local definitions capture missing or inaccurate components, inventory items, users, and assessment tools.

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

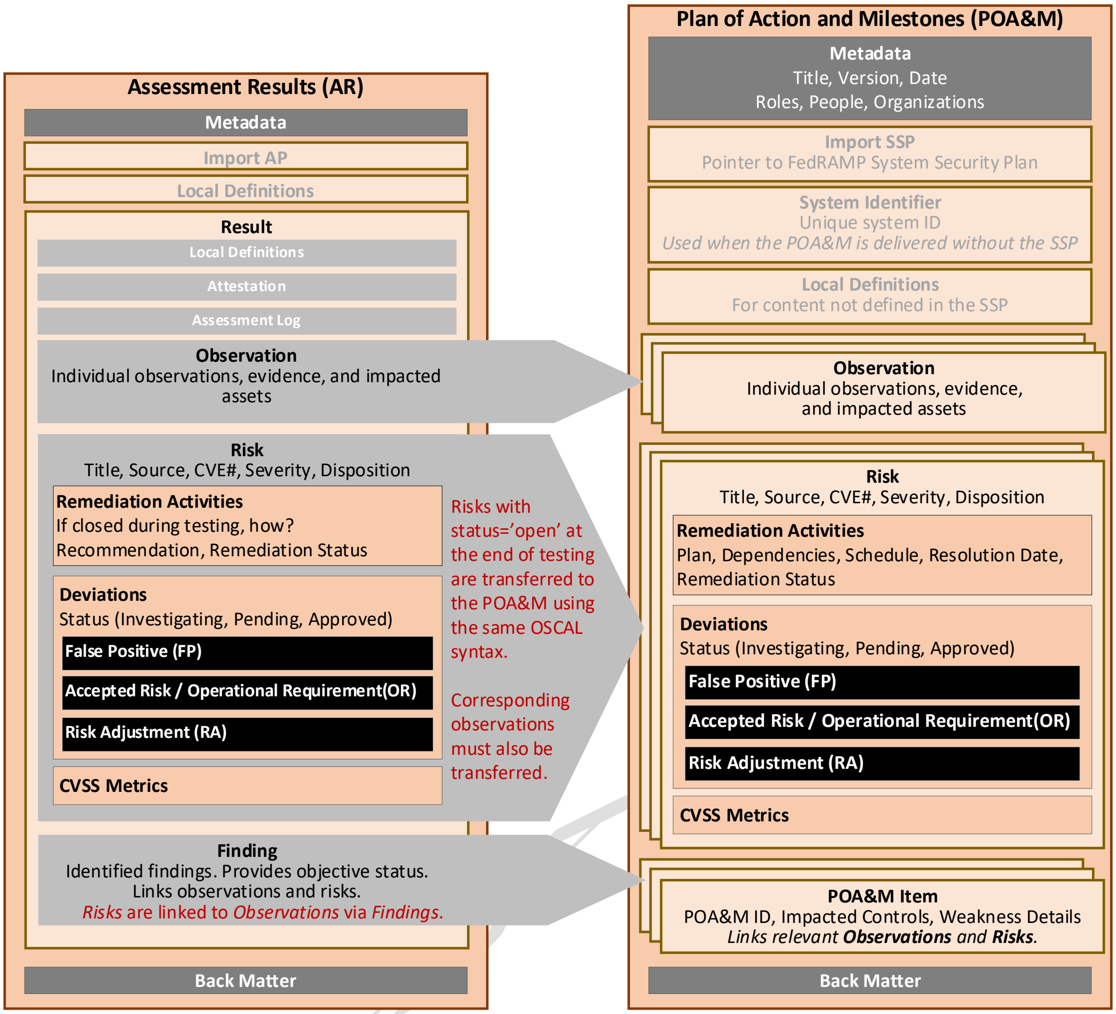
3.2.3. Copying SAR Residual Risks to the POA&M

FedRAMP requires residual risks from an initial or annual assessment to be reflected in the POA&M. The `observation` and `risk` assemblies syntax of the SAR and POA&M are identical to facilitate ease of transfer. The SAR `finding` assembly and POA&M `poam-item` assembly are also as similar as possible to further facilitate this transfer.

At the end of an assessment, copy all "`open`" risks from the SAR to POA&M. For every copied risk, also copy all related observations. Risks are linked to observations in the `finding` assembly.

If available, use the `finding/target` citation in the SAR to determine the impacted control and set the value in the risk section of the POA&M using the "`impacted-control`" FedRAMP Extension. If the identified SAR risk is not associated with a specific control, the SAR tool should prompt the assessor to assign a value for the risk in the resulting POA&M export.

It may also be necessary to copy content from the AP or SAR into the POA&M's Local Definitions, such as to ensure Observation/Origin references remain valid.


Assessment Results (AR)
Metadata
Import AP
Local Definitions
Result
Local Definitions
Attestation
Assessment Log
Observation
Individual observations, evidence, and impacted assets
Risk
Title, Source, CVE#, Severity, Disposition
Remediation Activities
If closed during testing, how?
Recommendation, Remediation Status
Deviations
Status (Investigating, Pending, Approved)
False Positive (FP)
Accepted Risk / Operational Requirement(OR)
Risk Adjustment (RA)
CVSS Metrics
Finding
Identified findings. Provides objective status.
Links observations and risks.
Risks are linked to Observations via Findings.
Back Matter
Risks with status='open' at the end of testing are transferred to the POA&M using the same OSCAL syntax.
Corresponding observations must also be transferred.
Plan of Action and Milestones (POA&M)
Metadata
Title, Version, Date
Roles, People, Organizations
Import SSP
Pointer to FedRAMP System Security Plan
System Identifier
Unique system ID
Used when the POA&M is delivered without the SSP
Local Definitions
For content not defined in the SSP
Observation
Individual observations, evidence, and impacted assets
Risk
Title, Source, CVE#, Severity, Disposition
Remediation Activities
Plan, Dependencies, Schedule, Resolution Date, Remediation Status
Deviations
Status (Investigating, Pending, Approved)
False Positive (FP)
Accepted Risk / Operational Requirement(OR)
Risk Adjustment (RA)
CVSS Metrics
POA&M Item
POA&M ID, Impacted Controls, Weakness Details
Links relevant Observations and Risks.
Back Matter

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

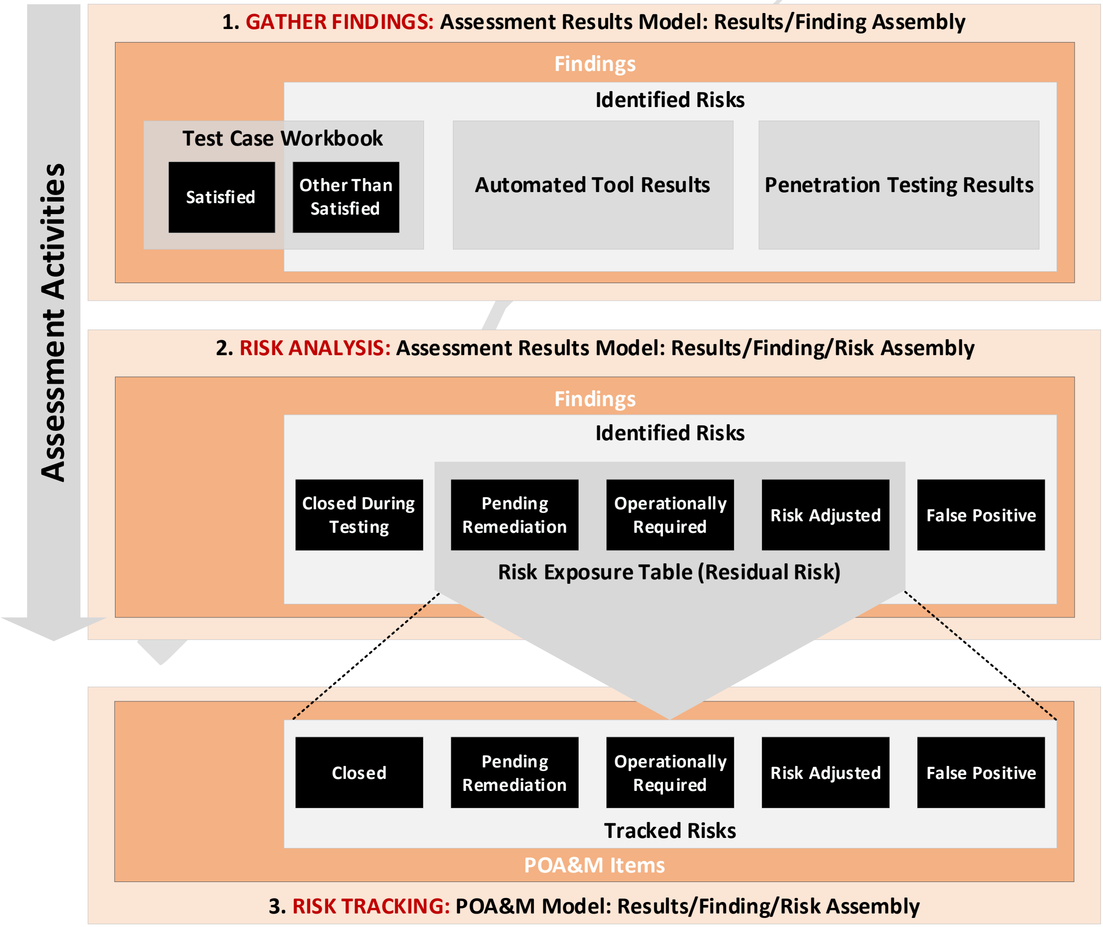
Ideally, tools will automatically detect potential duplicate risks between a new SAR and existing POA&M. In any case, tools should offer a mode for manual review and merging of duplicate risks from different sources.

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

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 Cloud Service Provider (CSP)'s POA&M.

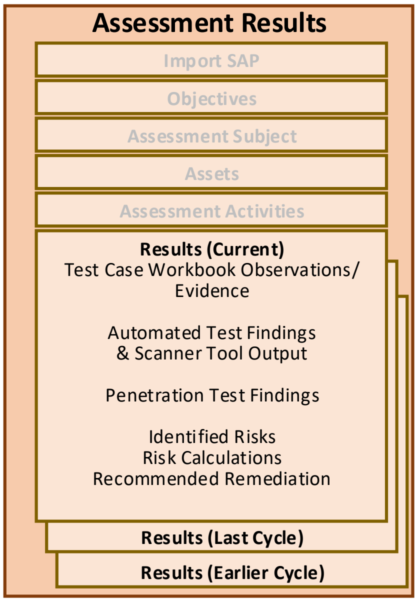


A SAR allows the assessor to update finding and risk information during the assessment.

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 result 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 result 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 result assembly

SAR Representation

```
    <result uuid="d2b54365-1b4c-427c-a42d-5ad2932a0a73">
        <title>2023 Annual Assessment</title>
        <description></description>
        <start>2023-03-01T00:00:00Z</start>
        <end>2023-03-12T00:00:00Z</end>
        <!-- findings -->
    </result>
    <result uuid="fcaa8260-8254-49d3-9ca2-751bacd4b715">
        <title>2022 Annual Assessment</title>
        <description></description>
        <start>2022-03-01T00:00:00Z</start>
        <end>2022-03-12T00:00:00Z</end>
        <!-- findings -->
    </result>
    <result uuid="6608034d-aa14-4c82-b60d-57dc5aeeecee">
        <title>2021 Initial Assessment</title>
        <description></description>
        <start>2021-03-01T00:00:00Z</start>
        <end>2021-03-12T00:00:00Z</end>
        <!-- findings -->
    </result>
```

XPath Queries

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

(SAR) Start Date of First Results Set:
  /*/result/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/dist/content/rev5/templates/sar/json/FedRAMP-SAR-OSCAL-Template.json
- OSCAL-based FedRAMP SAR Template (XML Format): https://github.com/GSA/fedramp-automation/raw/master/dist/content/rev5/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/concepts/layer/assessment/assessment-results/

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="#[uuid-value]" />
```

XPath Queries

```
(SAR) URI to SSP:
  /*/import-ap/@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 SAR 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="96445439-6ce1-4e22-beae-aa72cfe173d0">
        <title>[System Name] [FIPS-199 Level] SAP</title>
        <prop name="type" ns="https://fedramp.gov/ns/oscal" value="sap"/>
        <!-- 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>
```

XPath Queries

```
(SAR) Referenced OSCAL-based SAP:
  /*/back-matter/resource[@uuid='96445439-6ce1-4e22-beae-aa72cfe173d0']
  /rlink[@media-type= 'application/xml']/@href
```

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

3.6 Resolution Resource Prop

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

SSP Resolution Resource

```
<assessment-results>
   <metadata>
      <title>FedRAMP Security Assessment Results (SAR)</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 SAR (rev 4 or rev 5) this OSCAL 
document is for.</p>
         </remarks>
      </resource>

    </back-matter>
</ assessment-results>
```

XPath Queries

```
(SAR) UUID of “resolution-resource”:
  /*/metadata/prop[@name=”resolution-resource”]/@value

(SAR)Target baseline version:
  /*/back-matter/resource[@uuid=”uuid-of-resolution-
  resource”]/prop[@name=”dataset” and @class=”version”]/@value
```

If the `“resolution-resource”` prop is not specified in the `metadata` section of the SAR, FedRAMP will assume the SAR 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. 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 adds details that are unique to the SAR.

This section addresses the 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 content.

As described in *Section 0, 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.

5. FedRAMP Extensions and Allowed Values

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

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

As a result, FedRAMP-compliant OSCAL files are a combination of the core OSCAL syntax and extensions defined by FedRAMP. The *Guide to OSCAL-Based FedRAMP Content* describes the concepts behind FedRAMP extensions and allowed values. The extensions related to the Security Assessment Plan (SAP) are cited in this document in context of their use.

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

Revised FedRAMP Registry Approach

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

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

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*

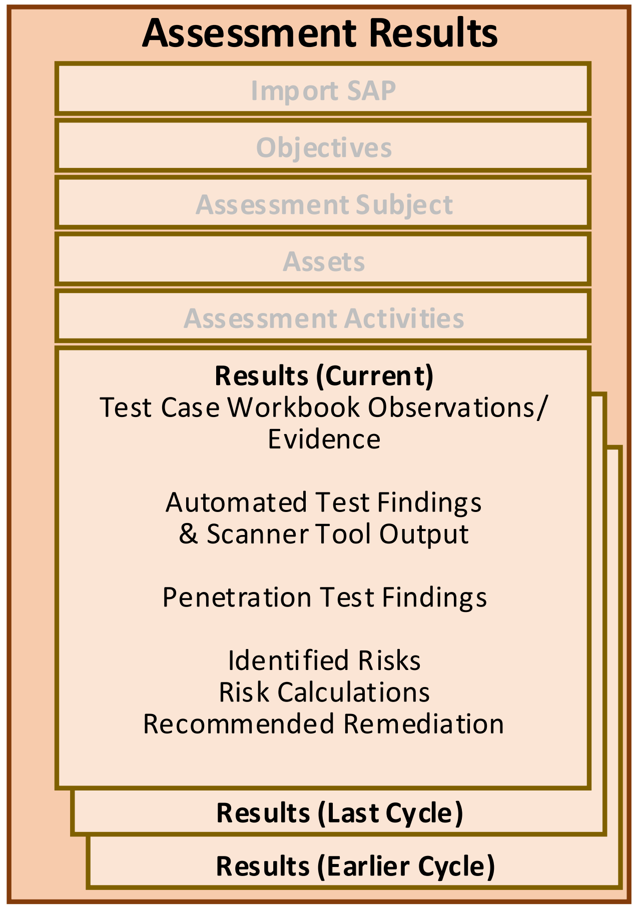
Record of Template Changes	Not Applicable. Instead follow *Guide to OSCAL-based FedRAMP Content, Section 2.3.2, OSCAL Syntax Version*
Revision History	*Guide to OSCAL-based FedRAMP Content, Section 4.5*
How to Contact Us	*Guide to OSCAL-based FedRAMP Content, Section 4.6*
Document Approvers	*Guide to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

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

- Any blue-text instructions found in the SSP template, where the instructions are related to the content itself.
- Table of Contents
- Introductory and instructive content in each section
- SAR Section 4.3, Consideration of Threats
- SAR Section 4.4, 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 result assembly

5.1. One Result Assembly for the Entire Assessment

All results from the current assessment, such as observations, findings, and risks, must be in a single `result` assembly. Additional `result` assemblies are used for past assessment results. One `result` 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 result assembly to determine the most recent set of results present in the SAR.

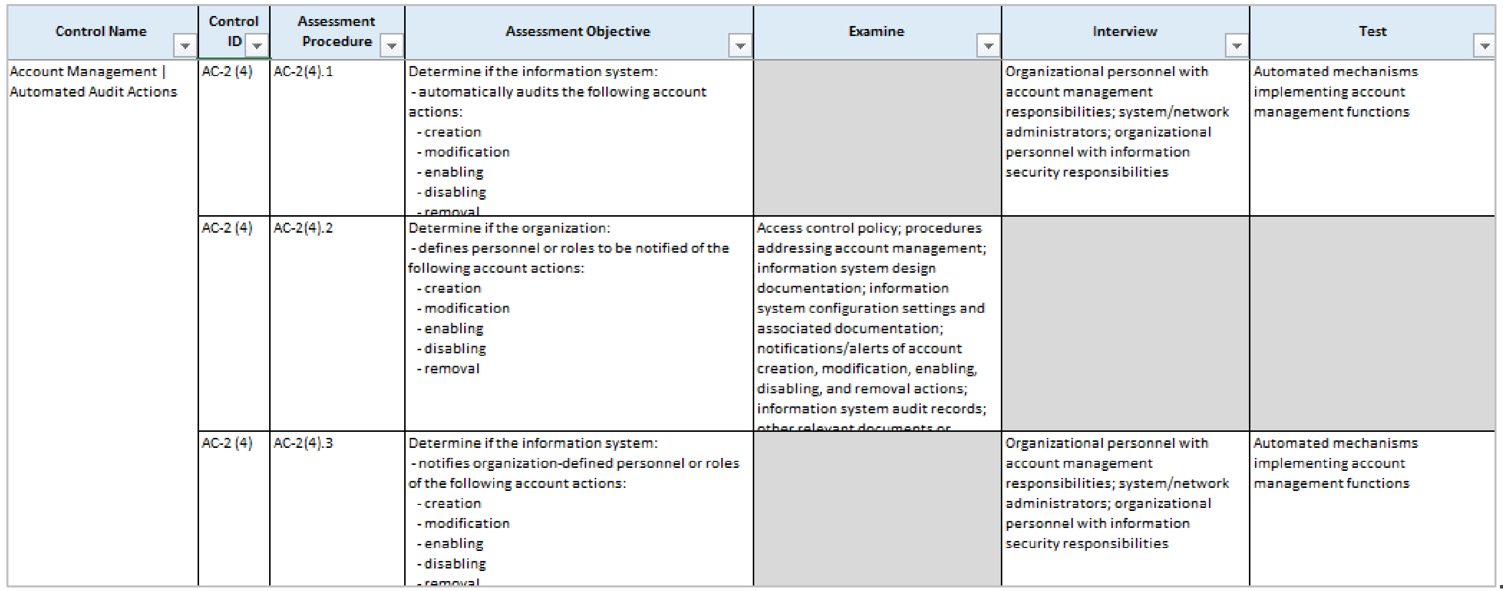
Representation

```
    <!-- assessment-activities -->
    <result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
        <title>2022 Annual Assessment</title>
        <description><p>Brief assessment description.</p></description>
        <start>2022-03-01T00:00:00Z</start>
        <end>2022-03-12T00:00:00Z</end>
        <!-- TCW Findings -->
        <!-- Penetration Test Findings -->
        <!-- Automated Testing / Scanner Findings -->
    </result>

    <result uuid="301a0bd4-18aa-4c3e-a4a8-07f544d27266">
        <title>2021 Annual Assessment</title>
        <description><p>Brief assessment description.</p></description>
        <start>2021-02-01T00:00:00Z</start>
        <end>2021-02-12T00:00:00Z</end>
        <!-- findings -->
    </result>

    <result uuid="74803987-0313-4bbd-9347-edfaa8364f46">
        <title>2020 Initial Assessment</title>
        <description><p>Brief assessment description.</p></description>
        <start>2020-01-01T00:00:00Z</start>
        <end>2020-01-12T00:00:00Z</end>
        <!-- findings -->
    </result>
    <!-- back-matter -->
```

XPath Queries

```
(SAR) Quantity of assessment cycles present in file:
  count(/*/result)
(SAR) Start date/time of first assessment cycle results in file:
  /*/result/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.



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

5.2. 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 2.1 of the Guide to OSCAL-based FedRAMP Content.

Within the OSCAL-based FedRAMP baselines, control statements and control objectives are tagged with a `response-point` FedRAMP Extension. For each **in-scope** control, every control objective designated as a `response-point` in the baseline must have a `finding` assembly in the `result` assembly of the SAR.

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

XPath Query

```
(Baseline) Response Points for AC-1:
  //control[@id='ac-1']/part[@name='objective']//prop[@name='response-point']
  [@ns='https://fedramp.gov/ns/oscal']/../@id
```

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

```
(Baseline) Response Points for AC Family:
  //group[@id='ac']/control/part[@name='objective']//prop[@name='response-point']
  [@ns='https://fedramp.gov/ns/oscal']/../@id
(Baseline) Response Points for entire baseline:
  //control/part[@name='objective']//prop[@name='response-point']
  [@ns='https://fedramp.gov/ns/oscal']/../@id
```

HELPFUL HINTS

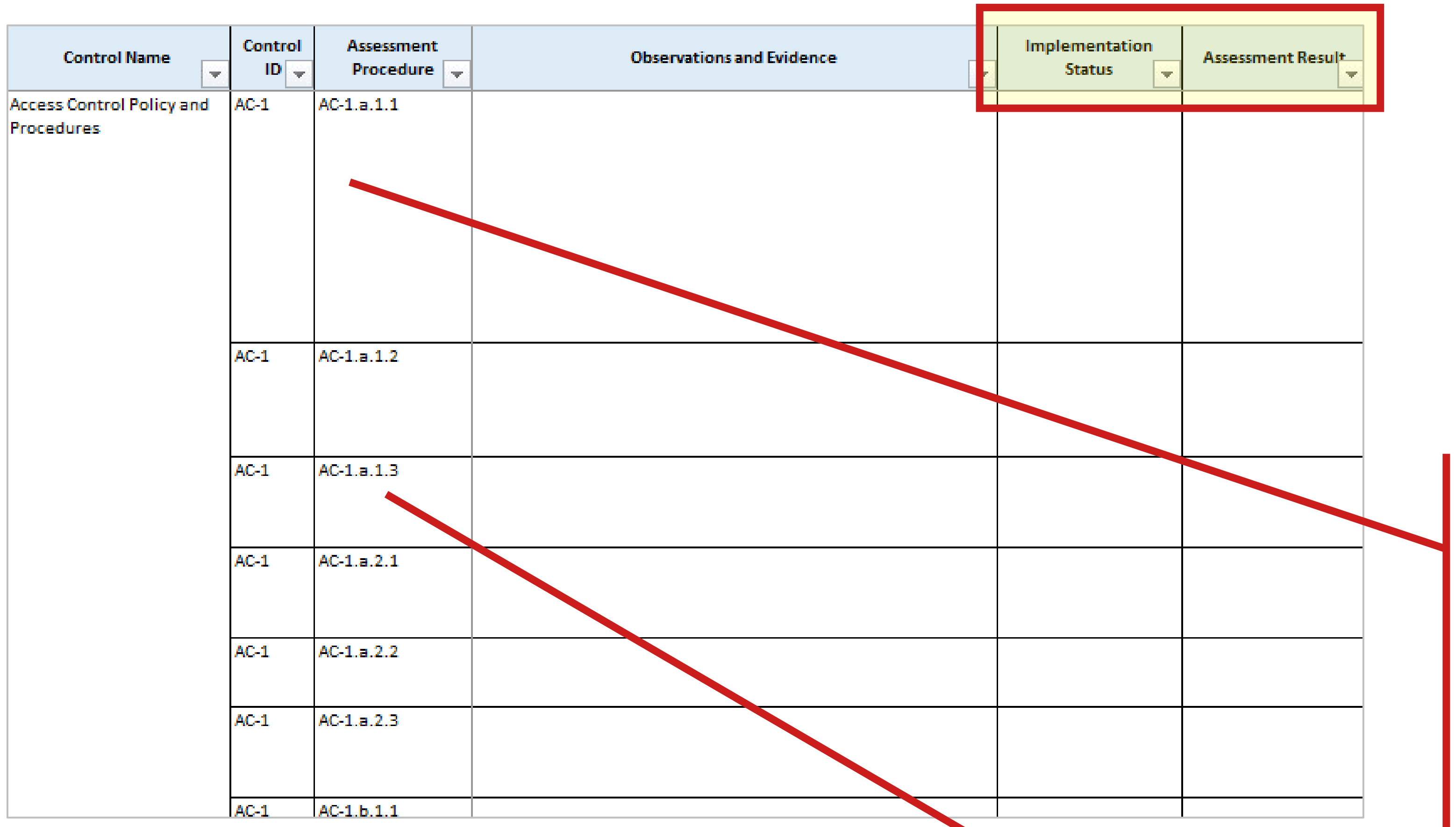
Use the appropriate FedRAMP resolved profile catalog, instead of the profile. This has the catalog content pre-merged, saving your tool the extra work of stepping through the profile to the catalog.

When processing an OSCAL-based FedRAMP baseline (profile or resolved-profile-catalog), each FedRAMP Test Case Workbook objective has a corresponding `part` named "`assessment-objective`" and part(s) named "`assessment-method`". The "`assessment-method`" parts have "`method`" properties specifying applicable assessment method (EXAMINE, INTERVIEW, TEST).

5.3. Test Case Workbook: Findings and Objective Status

There must be exactly one `finding` assembly for each required control objective as determined in the previous section. This is equivalent to having exactly one `finding` assembly for each in-scope row of the Excel-based FedRAMP TCW.

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



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			

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <!-- title, description, start, end -->
    <!-- local-definitions, reviewed-controls, assessment-log -->
    <!-- observation 1 -->
    <!-- observation 2 -->
    <!-- observation 3 -->
    <!-- risk A -->
    <!-- risk B -->
    <!-- risk C -->

    <finding uuid="951325ce-c0ca-4f8f-9b37-11ccf5258f3b">
        <title>[EXAMPLE]TCW Objective AC-1(a)(1)[1] <em>(Examine)</em></title>
        <description><p>Statement about satisfaction of this objective.</p>
          </description>
        <origin>
            <!-- Assessor POCs for this objective -->
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <actor type="party" actor-uuid="e934d8b5-13e5-4f77-b55e-871e6f2df2fe" />
        </origin>
        <target type="objective-id" target-id="ac-1.a.1_obj.1">
            <prop name="implementation-status" ns="https://fedramp.gov/ns/oscal"
value="implemented"/>
            <status reason="pass">satisfied</status>
        </target>
        <related-observation observation-uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab"/>
        <related-observation observation-uuid="29e4ce70-6a17-411d-aa65-ec7cef21e774"/>
        <associated-risk risk-uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9"/>
    </finding>

    <finding uuid="EF489684-C2E5-46BD-887A-A86A4AA210D9">
        <title>[EXAMPLE]TCW Objective AC-1(a)(1)[2] <em>(Examine)</em></title>
        <description><p>Statement about satisfaction of this objective.</p>
          </description>
        <origin>
            <!-- Assessor POCs for this objective -->
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <actor type="party" actor-uuid="e934d8b5-13e5-4f77-b55e-871e6f2df2fe" />
        </origin>
        <target type="objective-id" target-id="ac-1.a.1_obj.2">
```

Accepted Values

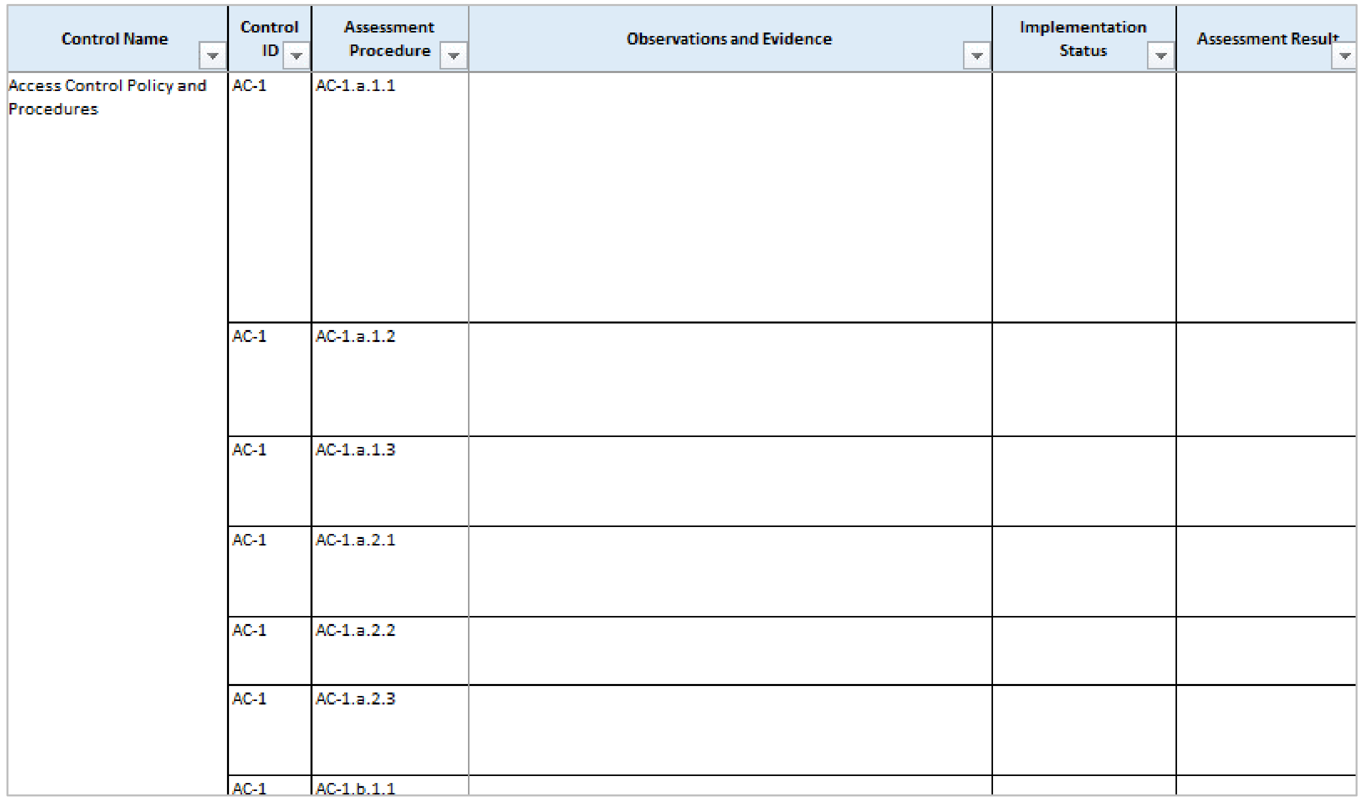
- The `implementation-status` fields must have the @ns flag with a value of https://fedramp.gov
- The `implementation-status` field may only have one of the following values, which match the SSP accepted values:
  - **`implemented, partial, planned, alternative, not-applicable`**
- The `status` field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

```
            <prop name="implementation-status" ns="https://fedramp.gov/ns/oscal"
value="implemented"/>
            <status reason="pass">satisfied</status>
        </target>
        <related-observation observation-uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab"/>
        <related-observation observation-uuid="29e4ce70-6a17-411d-aa65-ec7cef21e774"/>
        <associated-risk risk-uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9"/>
    </finding>

</result>
```

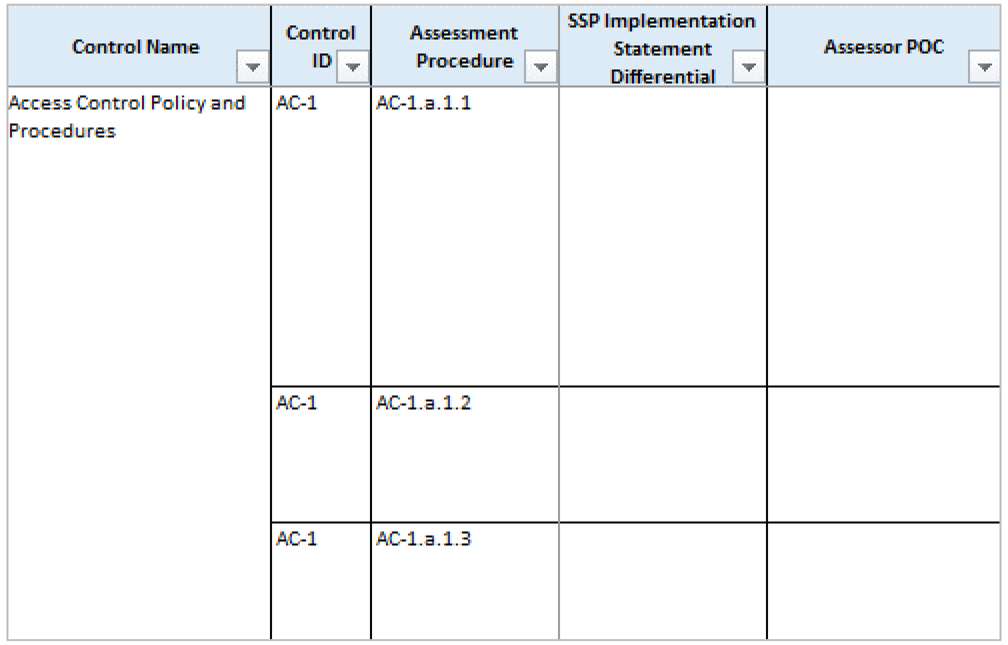
The assessors who gathered the evidence are identified at the bottom of the finding assembly using the `actor-uuid` attribute of the origin `actor` fields. The assessment team is defined as a `party` in the SAP `metadata`. If the assessor was not listed in the SAP, add a `party` to the SAR `metadata` 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.

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



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			



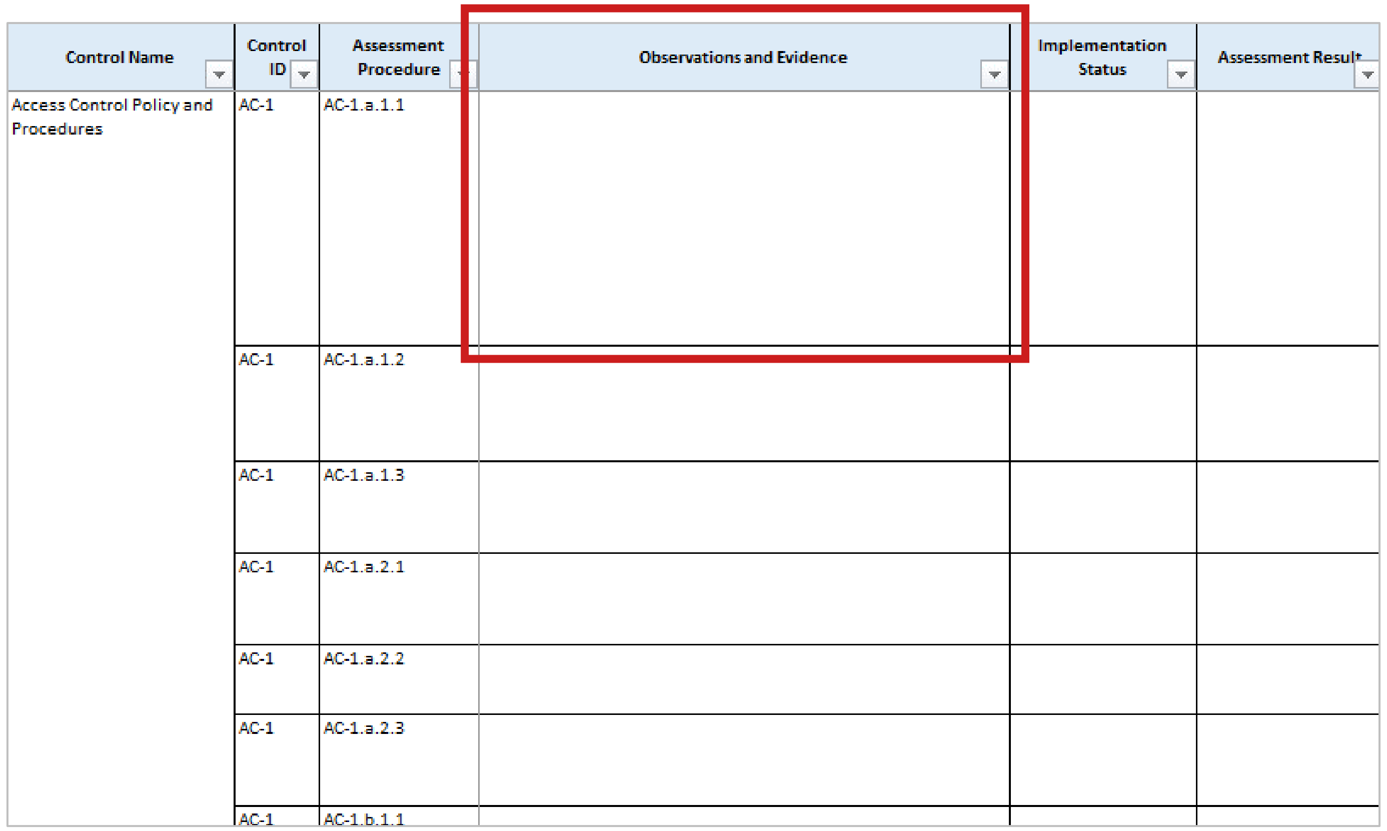
Control Name	Control ID	Assessment Procedure	SSP Implementation Statement Differential	Assessor POC
Access Control Policy and Procedures	AC-1	AC-1.a.1.1		
	AC-1	AC-1.a.1.2		
	AC-1	AC-1.a.1.3		

The following assumes, the first `result` assembly contains the current assessment, as determined in *Section 5.1, One Result Assembly for the Entire Assessment*.

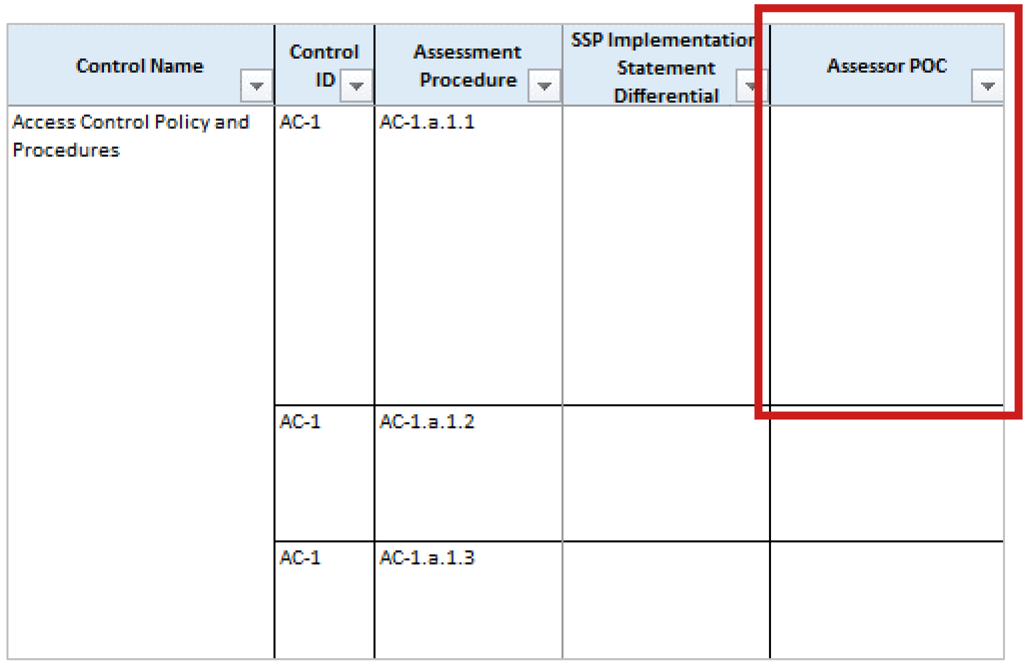
XPath Queries

```
(SAR) Implementation Status:
  /*/result[1]/finding/target[@type='objective-id'][@target-id='ac-1.a.1_obj.1']
  /prop[@name='implementation-status'][@ns='https://fedramp.gov/ns/oscal']
(SAR) Assessment Result:
  /*/result[1]/finding/target[@type='objective-id'][@target-id='ac-1.a.1_obj.1'] /status
(SAR) Quantity of Assessor POC's cited for this objective (integer):
  count(/*/result[1]/finding[./target[@type='objective-id'][@target-id='ac-
  1.a.1_obj.1'] ]/origin/actor[@type='party'])
(SAR) UUID of the First Assessor POC cited for this objective:
  /*/result[1]/finding[./target[@type='objective-id'][@target-id='ac-
  1.a.1_obj.1'] ]/origin/actor[@type='party'][1]/@actor-uuid
NOTE: Search the SAP and SAR metadata for the party referenced by the UUID.
```

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/reference/datatypes/#markup-multiline



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		

5.4. Test Case Workbook: Observations and Evidence

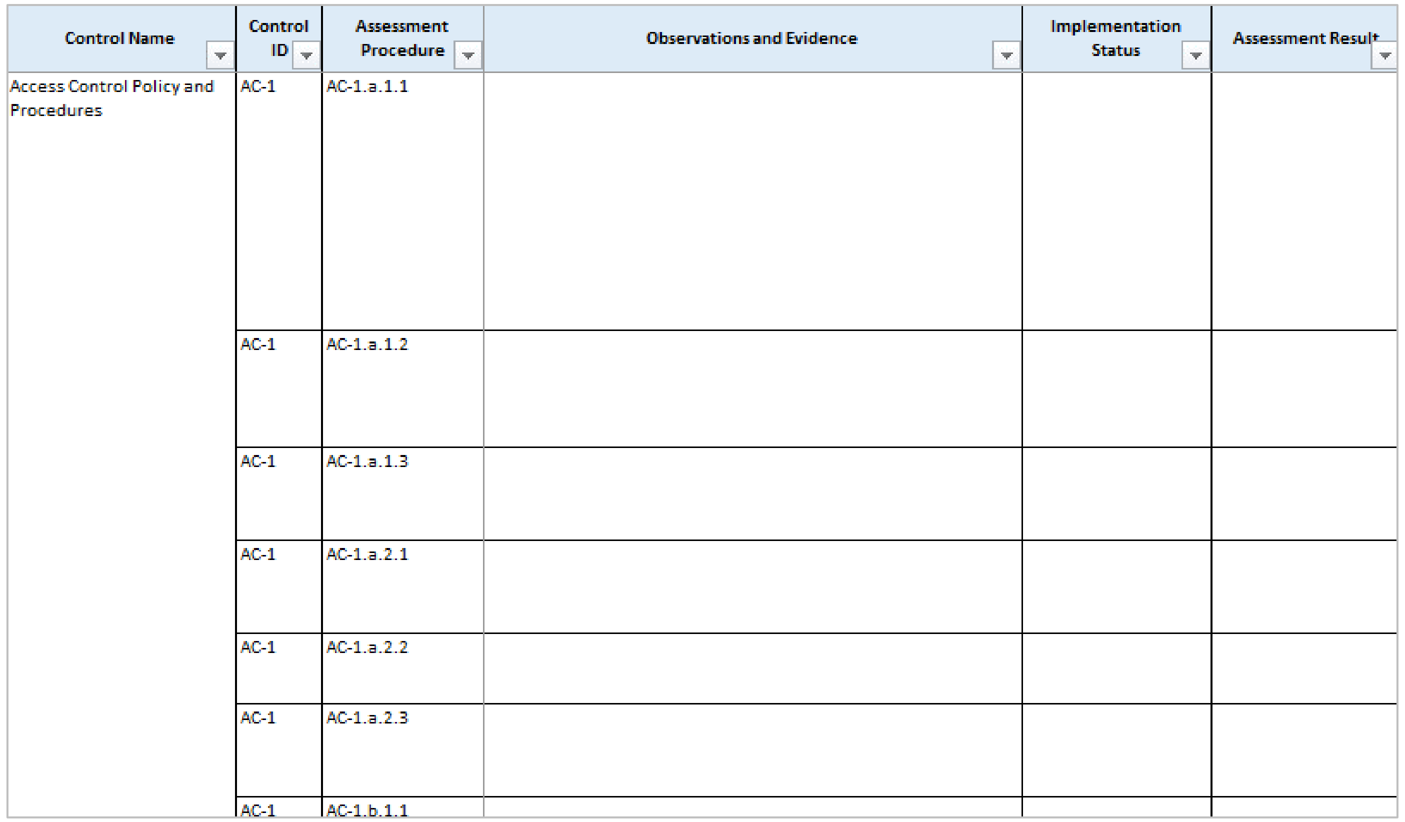
The historic TCW spreadsheet only provided the assessor one cell for each Assessment Procedure to capture all observations and evidence. OSCAL enables observations to be broken down into more granular detail, which further enables machine processing.

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 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?	`method (="EXAMINE", "INTERVIEW", "TEST")`
Categorize	`type [="control-objective"]`
Actor: Who performed this action?	`assessor`
Subject: Who was Interviewed?	`subject [type="party"]`
Subject: What was tested/inspected?	`subject [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 contain specific examples of Observations and Evidence.

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



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 type field must be set to:

- **control-objective**

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

- **EXAMINE, INTERVIEW, or TEST**

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

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

The type flag of the origin/actor field may be set to one of the following:

- **tool, party, assessment-platform**

5.4.1. 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 method is set to "EXAMINE" indicating this is in response to the EXAMINE activities prescribed for this objective.

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

The origin/actor field points to an individual identified as a party in the metadata assembly of either the SAP or SAR.

The origin/related-task points to the task in the SAP schedule (or locally defined task), which describes the review of documentation.

The subject cites 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.

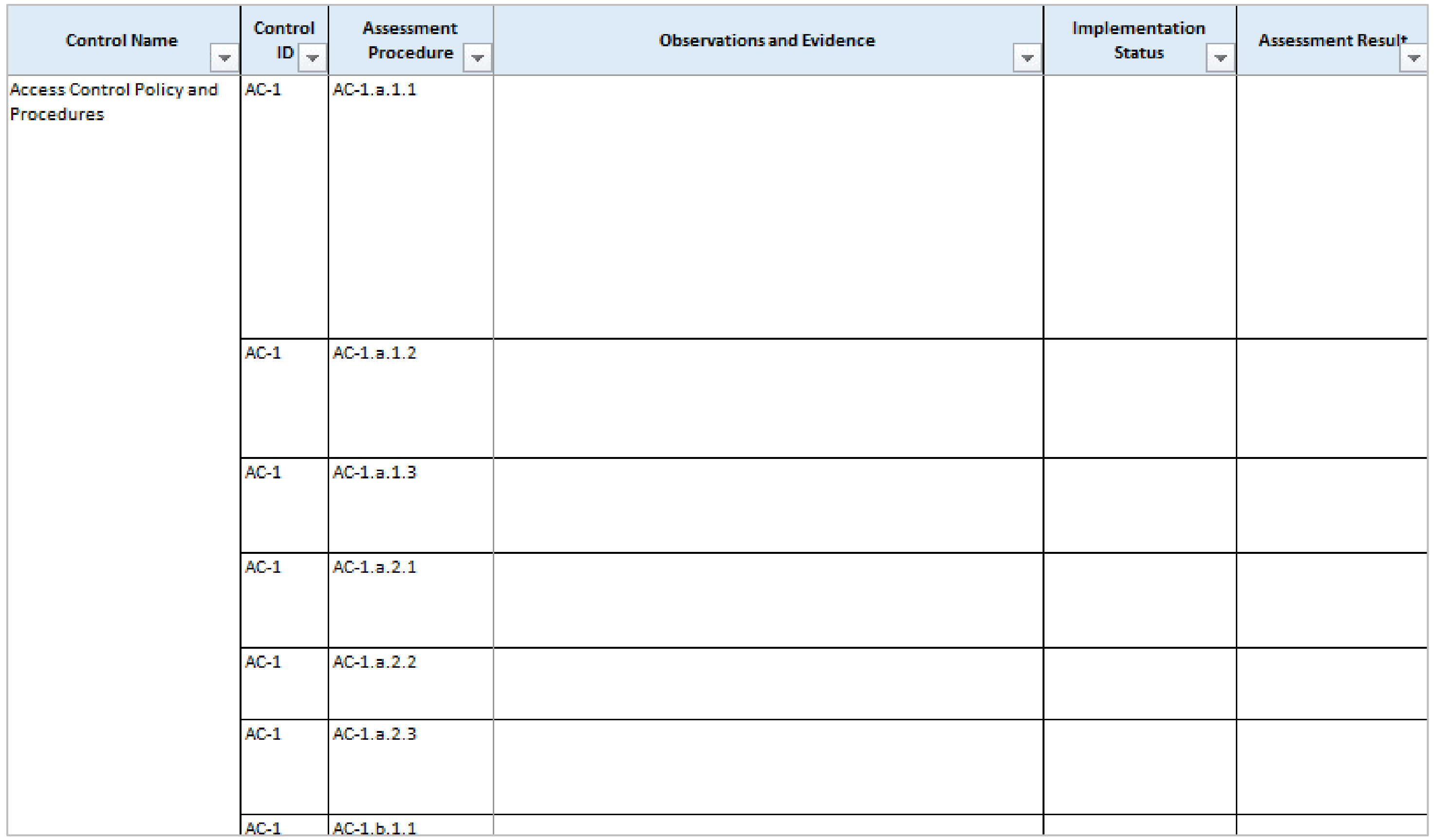
Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <!-- title, description, start, end -->
    <observation uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab">
        <title>[EXAMPLE]Examine AC Policy</title>
        <description>
            <p>[EXAMPLE]The AC policy existed, and had all the required elements.</p>
        </description>
        <method>EXAMINE</method>
        <type>control-objective</type>
        <origin>
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <related-task task-uuid="e1890486-a9f0-4388-b2bc-34fb6c623686" />
        </origin>
        <subject type="component" subject-uuid="f32b7ab1-baf1-451a-b3a1-1dfdadbe8dc7">
            <title>Reviewed Policy</title>
            <remarks>
                <p>If the policy is defined in the SSP as a component.</p></remarks>
        </subject>
        <relevant-evidence>
            <description><p>Reviewed Policy</p></description>
            <link href="#f32b7ab1-baf1-451a-b3a1-1dfdadbe8dc7" rel="policy" />
            <remarks><p>If the policy is <em>not</em> an SSP component.</p></remarks>
        </relevant-evidence>
        <collected>2020-10-10T00:00:00Z</collected>
    </observation>
```

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

```xml
    <observation uuid="29e4ce70-6a17-411d-aa65-ec7cef21e774">
        <!-- method: INTERVIEW -->
    </observation>

    <!-- risk A -->
    <finding uuid="30f81987-b773-4034-a54d-a75753cb5464">
        <!-- findings risks to observations -->
        <related-observation observation-uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab"/>
        <related-observation observation-uuid="29e4ce70-6a17-411d-aa65-ec7cef21e774"/>
    </finding>
</result>
```

Finally, the `relevant-evidence` assembly is used to reference evidence. It has an optional `href` flag that is used to reference a backmatter resource. Alternatively, the `relevant-evidence` assembly has a child `link` field then can also be used to reference a backmatter resource. Either approach is acceptable, however if both `relevant-evidence/@href` and `relevant-evidence/link/@href` are specified, the `link` is assumed to be the definitive reference. The previous example demonstrates using `link` to point back to an examined policy document.



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 `type` field must be set to:

- **`control-objective`**

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

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

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

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

The `type` flag of the `origin/actor` field may be set to one of the following:

- **`tool, party, assessment-platform`**

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

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

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

The `origin/related-task` points to the task in the SAP schedule (or locally defined in the SAR), which describes the interviewing of staff.

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

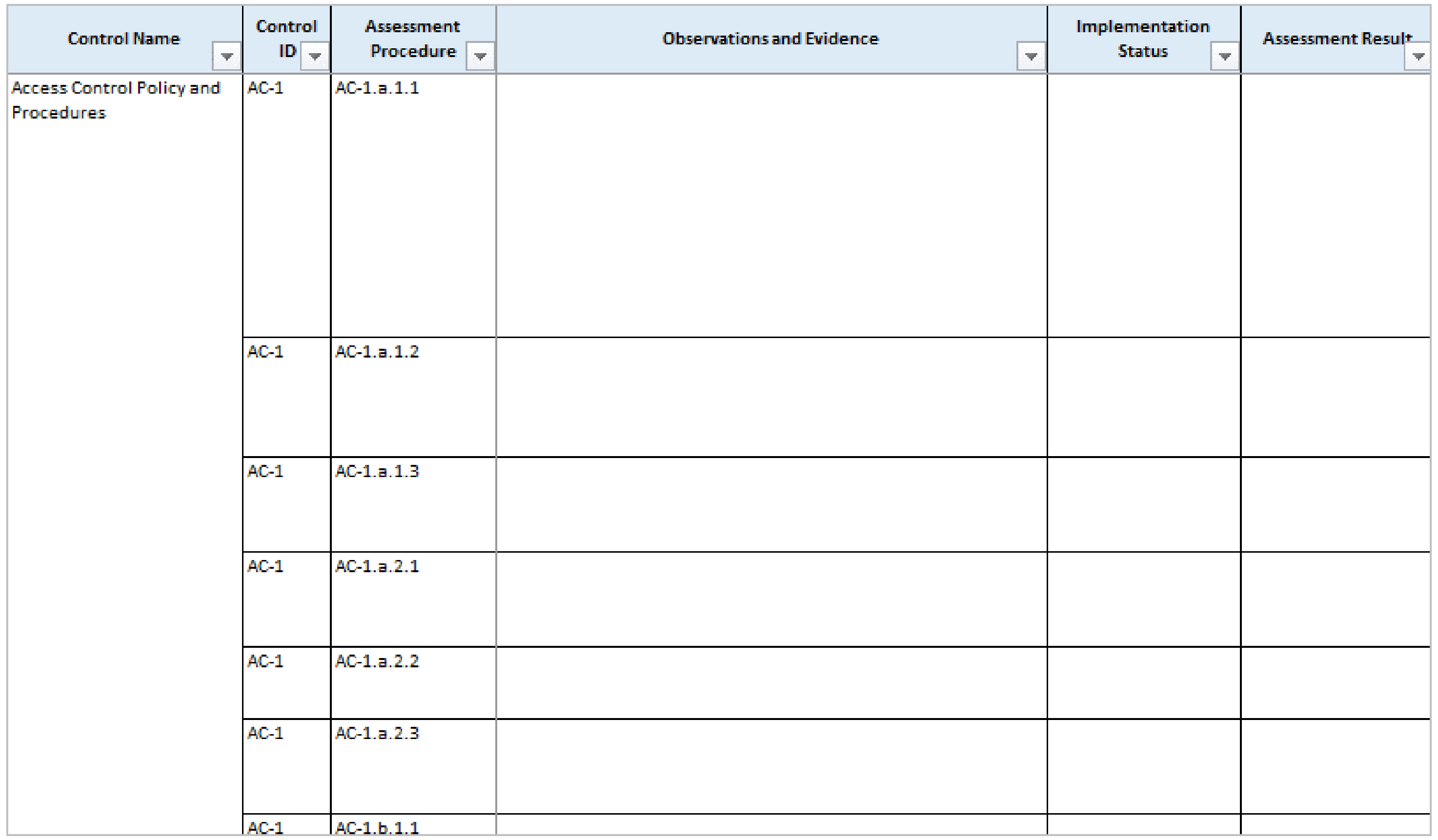
Finally, the `relevant-evidence` must be used to point to the attached interview notes as a URI fragment, and to provide detail as to where the relevant statements are in the notes. While OSCAL will allow a relative external link in the `href` flag, FedRAMP requires each piece of evidence to be listed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

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <!-- title, description, start, end -->
    <observation uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab">
        <!-- method: EXAMINE -->
    </observation>

    <observation uuid="29e4ce70-6a17-411d-aa65-ec7cef21e774">
        <title>[EXAMPLE]AC Policy Interview</title>
        <description>
            <p>[EXAMPLE]The person interviewed knew about the policy and where to find
it.</p>
        </description>
        <method>INTERVIEW</method>
        <type>control-objective</type>
        <origin>
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <related-task task-uuid="172d4ba2-3362-4e3b-9379-a65a50e399bf" />
        </origin>
        <subject type="party" subject-uuid="5ff3d794-d2e8-48be-bf9c-95c2328271ce">
            <title>Interviewed Person</title>
        </subject>
        <relevant-evidence href="#65fb91b1-f7dc-46bf-8b99-bd98f1a5293d">
```

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

```
            <description><p>describe the evidence.</p></description>
        </relevant-evidence>
        <collected>2020-10-10T00:00:00Z</collected>
    </observation>

    <!-- risk A -->
    <finding uuid="30f81987-b773-4034-a54d-a75753cb5464">
        <!-- cut -->
        <related-observation observation-uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab"/>
        <related-observation observation-uuid="29e4ce70-6a17-411d-aa65-ec7cef21e774"/>
    </finding>
</result>
```



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			

5.4.3. TCW - Observations and Evidence: Evidence and Artifacts

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

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

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

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

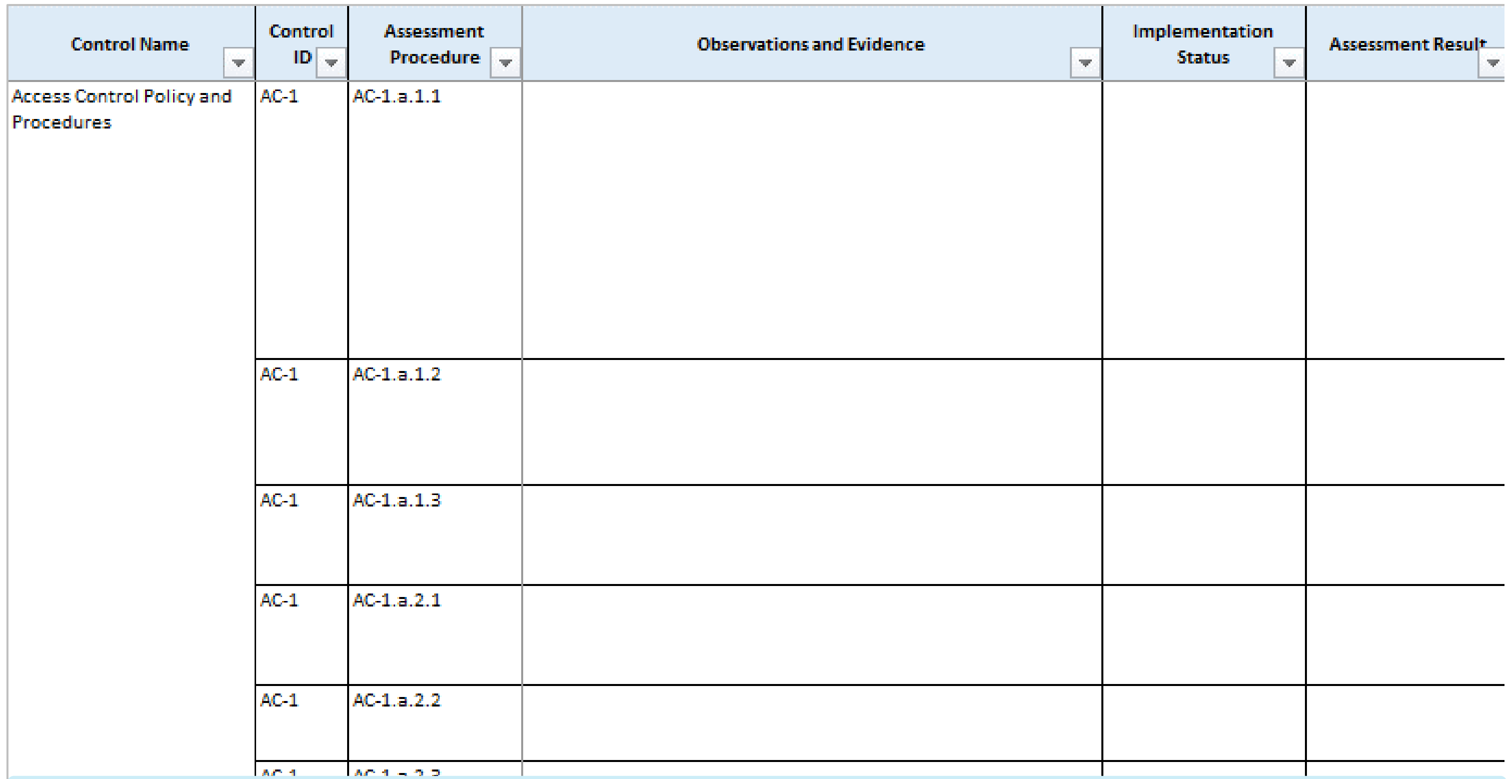
Artifacts and evidence may be cited from an `observation` as `relative-evidence`.

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 within the same `resource` assembly. This may be useful if the 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" value="evidence"/>
        <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" value="artifact"/>
        <prop name="type" value="policy"/>
        <prop name="version" value="2.1"/>
        <prop name="publication" value="2018-11-11T00:00:00Z"/>
        <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" value="evidence"/>
        <rlink media-type="image/jpeg" href="./evidence/screen-shot.jpg"></rlink>
        <base64 media-type="image/jpeg" 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			

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 `subject-uuid` value identified by `subject` 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 `related-evidence` 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.

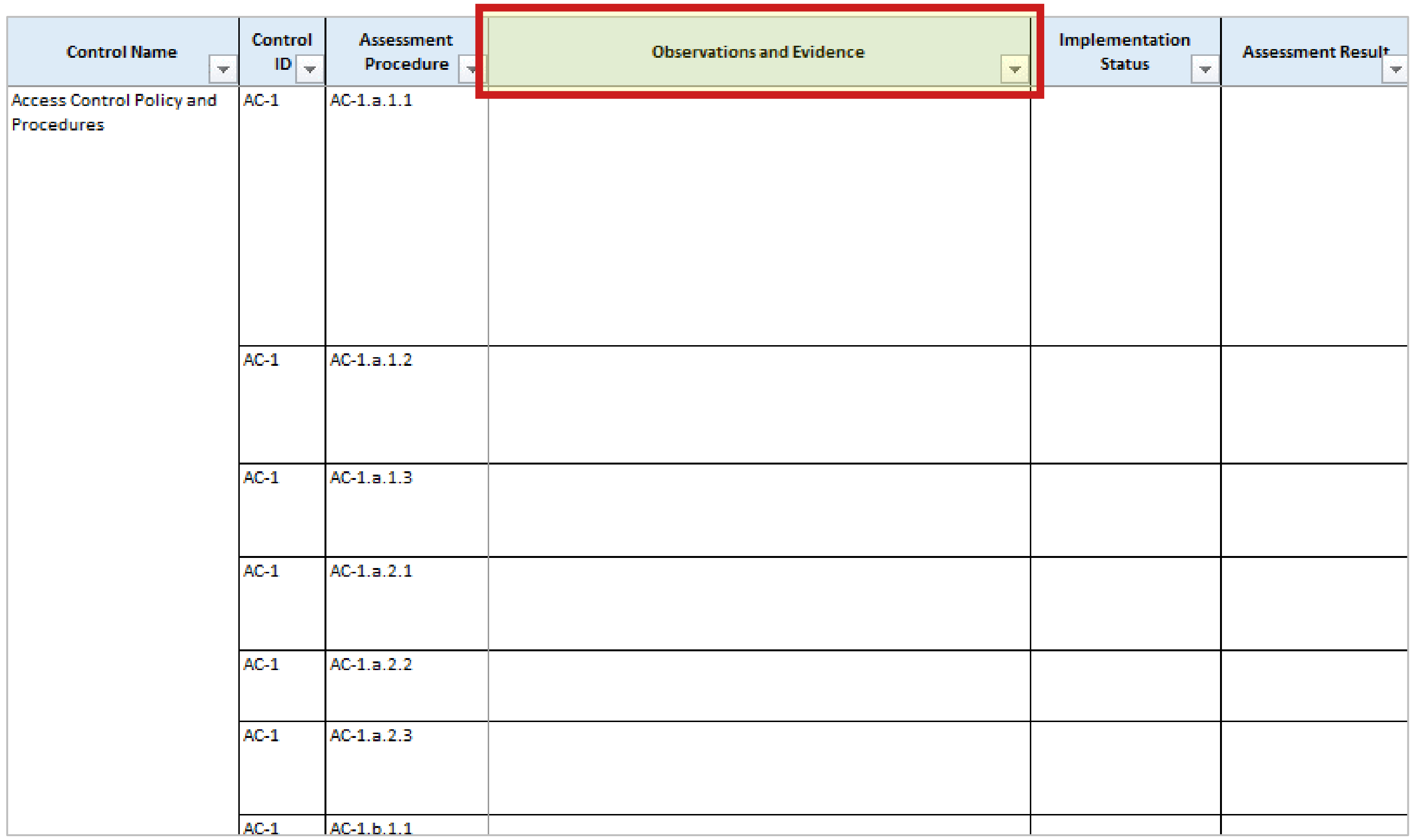
The `description` fields are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline

5.4.4. TCW - Observations and Evidence: Queries

The following assumes, the first `result` assembly contains the current assessment, as determined in *Section 5.1, One Result Assembly for the Entire Assessment*.

XPath Queries

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

(SAR) The second observation for this objective:
  /*/result[1]/observation[@uuid=/*/result[1]/finding[./target[@type='objective-id'][@
  target-id='ac-1.a.1_obj.1']]/related-observation[1]/@observation-
  uuid]/description/node()

(SAR) SOURCE: Type of source cited (first finding, first, observation, first source):
  /*/result[1]/observation[@uuid=/*/result[1]/finding[./target[@type='objective-id'][@
  target-id='ac-1.a.1_obj.1']]/related-observation[1]/@observation-
  uuid]/origin/actor/@type

(SAR) SOURCE: UUID of source cited (first finding, first, observation, first source):
  /*/result[1]/observation[@uuid=/*/result[1]/finding[./target[@type='objective-id'][@
  target-id='ac-1.a.1_obj.1']]/related-observation[1]/@observation-
  uuid]/origin/actor/@actor-uuid

(SAR) SUBJECT: Type of subject cited, such as interviewed people or examined/tested
  system components:
  /*/result[1]/observation[@uuid=/*/result[1]/finding[./target[@type='objective-id'][@
  target-id='ac-1.a.1_obj.1']]/related-observation[1]/@observation-uuid]/subject/@type

(SAR) SUBJECT: UUID of subject cited, such as interviewed people, examined/tested system
  components, or reviewed artifacts:
  /*/result[1]/observation[@uuid=/*/result[1]/finding[./target[@type='objective-id'][@
  target-id='ac-1.a.1_obj.1']]/related-observation[1]/@observation-uuid]/subject/@actor-
  uuid

(SAR) EVIDENCE: Description of the first piece of evidence for the second observation:
  /*/result[1]/observation[@uuid=/*/result[1]/finding[./target[@type='objective-id'][@
  target-id='ac-1.a.1_obj.1']]/related-observation[1]/@observation-uuid]/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:
  /*/result[1]/observation[@uuid=/*/result[1]/finding[./target[@type='objective-id'][@
  target-id='ac-1.a.1_obj.1']]/related-observation[1]/@observation-uuid]/relevant-
  evidence/link/@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` fields are *Markup multiline*, which enables the text to be formatted. See the *[Guide to OSCAL-based FedRAMP Content](#), Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/reference/datatypes/#markup-multiline

5.4.5. 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 legacy 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 `result` 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 sections 4.3 – 4.4.4.

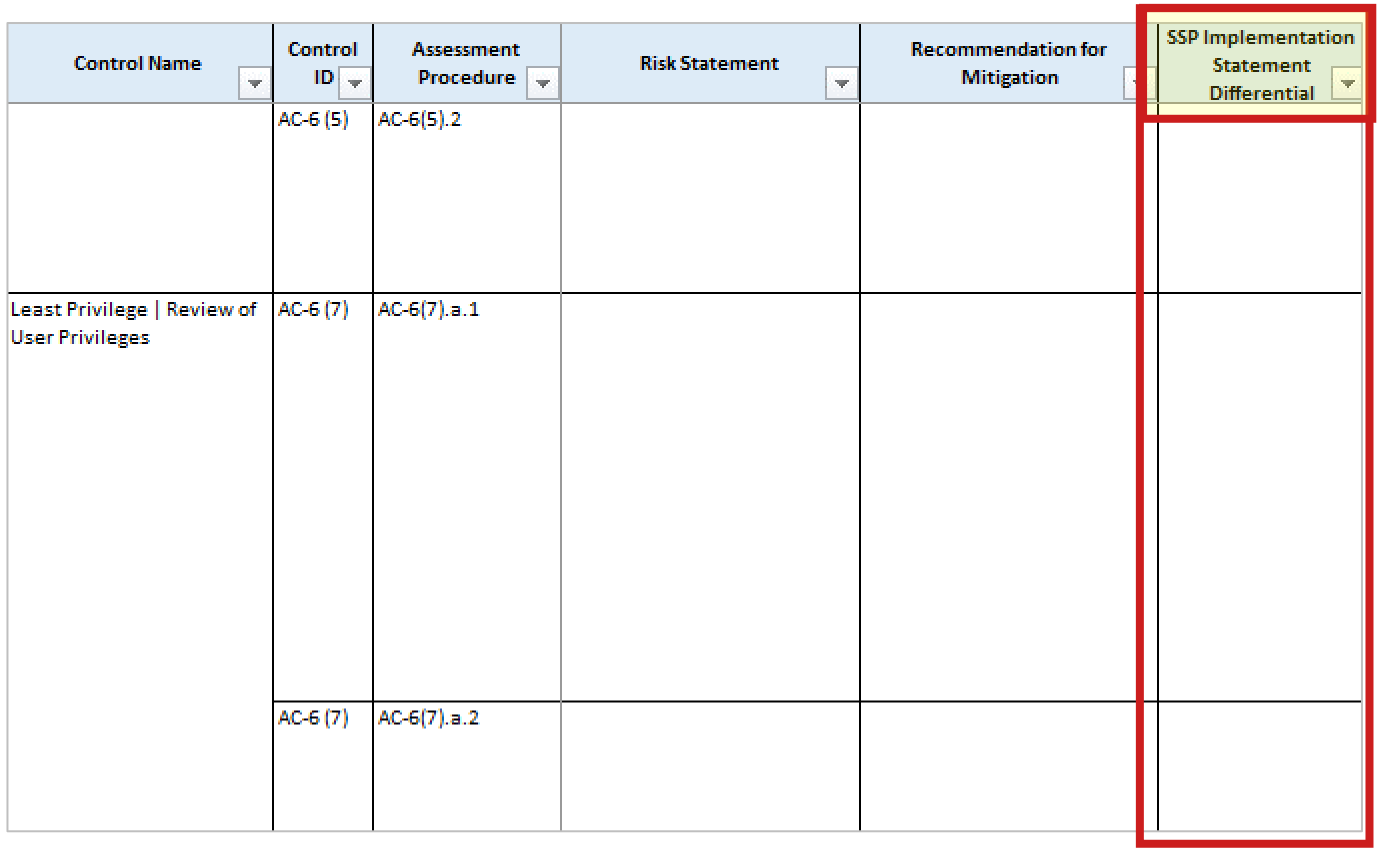
Representation

```
<result uuid="d755e7fd-346d-40f0-b538-1b1da1aa5821">
    <title>Initial (2018) Assessment</title>
    <description/>
    <start>2022-03-01T00:00:00Z</start>
    <end>2022-03-12T00:00:00Z</end>

    <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>
        <method>MIXED</method>
        <type>historic</type>
        <origin>
            <actor type="party" actor-uuid=" e934d8b5-13e5-4f77-b55e-871e6f2df2fe" />
        </origin>
        <collected>2022-03-01T00:00:00Z</collected>

    </observation>

    <finding uuid="0cbd1819-3ea7-4f78-9ebc-92873eab4d6e">
        <title>AC-1.1.1.3</title>
        <description/>
        <target type="objective-id" target-id="ac-1.1_obj.3">
            <prop name="implementation-status"
                ns="https://fedramp.gov/ns/oscal" value="implemented"/>
            <status>satisfied</status>
        </target>
    </finding>
    <!-- finding -->
    <!-- finding -->
</result>
```

5.5. Test Case Workbook: SSP Implementation Statement Differential

If an SSP Implementation Statement Differential is identified, add an additional `observation` with a `type` value of "`ssp-statement-issue`" and cite this observation from `finding` assembly. The finding assembly should also include the `implementation-statement-uuid` field with the UUID of the original statement in the SSP.

If this was an issue where an inventory-item or component was not configured as described in the SSP, the related observation should include the relevant inventory-item or component should be cited as subjects.



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 `type` field must be set to:

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

The observation `method` field must be set to:

- **`EXAMINE`**

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

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

The `type` flag of the `origin/actor` field may be set to one of the following:

- **`tool, part, or assessment-platform`**

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">

    <observation uuid="a38f3bba-5b71-400d-b8f2-d808e1d4627f">
        <description><p>Policy describes procedure, which could not be
found.</p></description>
        <method>EXAMINE</method>
        <type>ssp-statement-issue</type>
        <origin>
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
        </origin>
        <collected>2022-10-10T00:00:00Z</collected>
    </observation>

    <finding uuid="33e43825-6fd7-49c6-a610-4c795954a167">
        <title>[EXAMPLE]Issue With AU-1 Statement</title>
        <description><p>[EXAMPLE]There is an issue with an SSP
Statement.</p></description>
        <origin>
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <actor type="party" actor-uuid="e934d8b5-13e5-4f77-b55e-
871e6f2df2fe"></actor>
        </origin>
        <implementation-statement-uuid
            >7924db51-e44d-4215-ad7e-3a5dda44a631</implementation-statement-uuid>
        <related-observation observation-uuid="a38f3bba-5b71-400d-b8f2-d808e1d4627f" />
    </finding>
</result>
```

The following assumes, the first `result` assembly contains the current assessment, as determined in *Section 5.1, One Result Assembly for the Entire Assessment*.

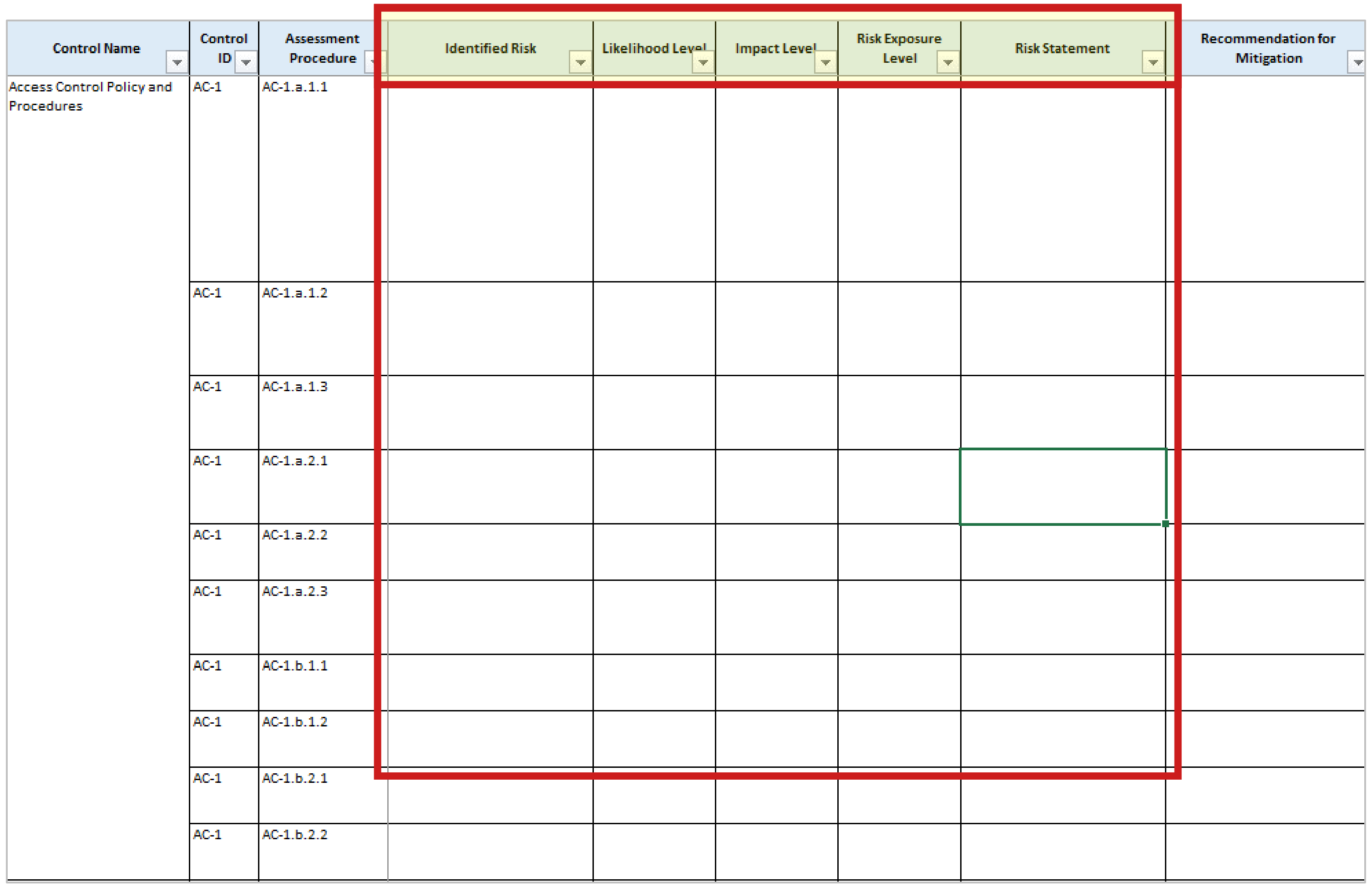
XPath Queries

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

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

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

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

5.6. Test Case Workbook: Identified Risks



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 risk `status` field should always be set to "`open`" when a risk content is first created.
- The facet `likelihood` and `impact` fields must each have one of the following values:
  - **`low`**
  - **`moderate`**
  - **`high`**
- The risk exposure rating 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

For any finding with a `finding/target/status` value of "`not-satisfied`", there must be at least one `associated-risk` field within the `finding` assembly, pointing to a `risk` assembly.

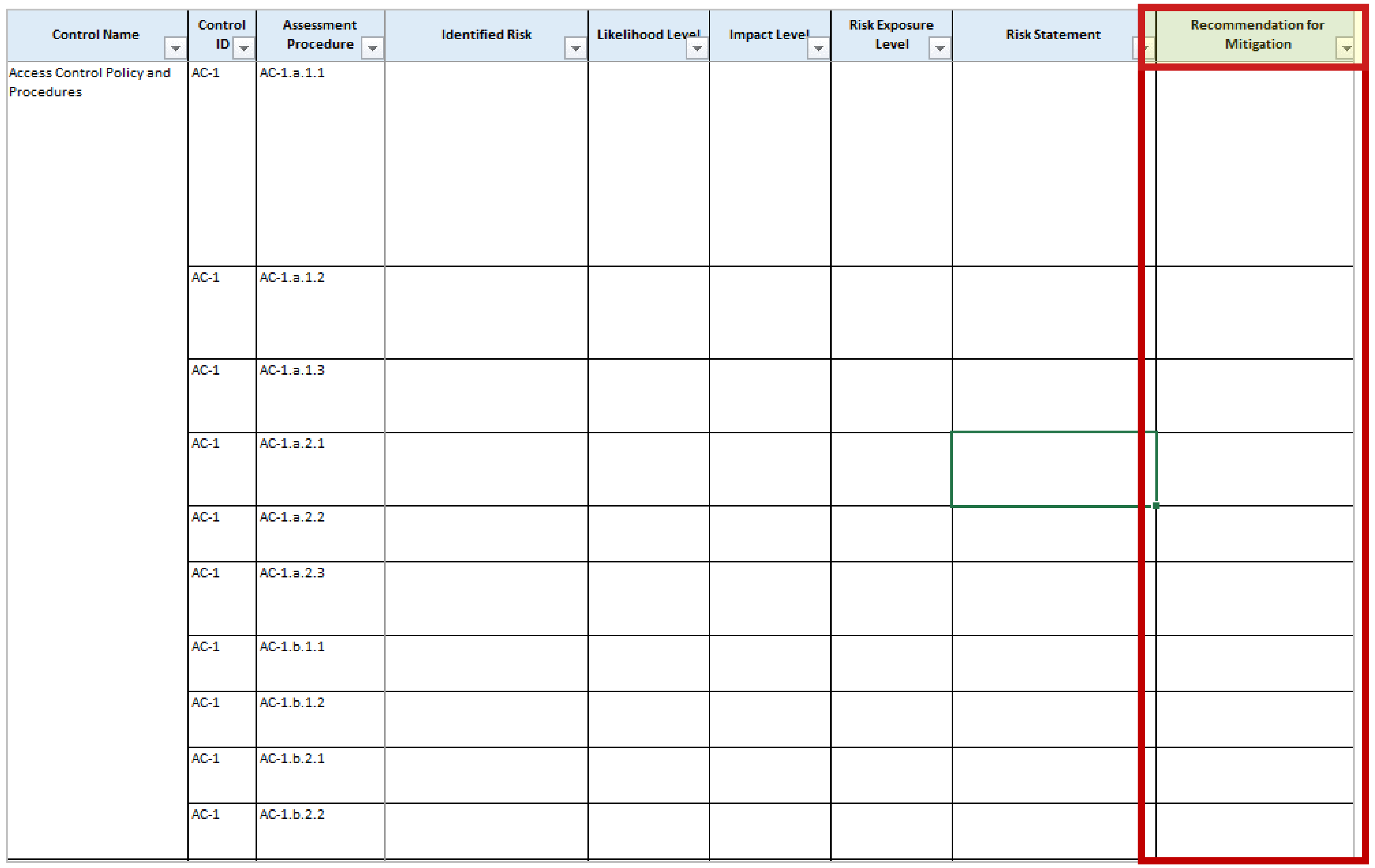
Within the cited risk assembly, the "Identified Risk" is described in the `description` field. The Risk Statement is described in the `risk-statement` field.

The Likelihood Level and Impact Level are each entered in a `characterization/facet` field. The FedRAMP Risk Exposure Level must be calculated by the SAR tool. If the "`state`" annotation is missing, it is assumed to be "`initial`".

Initially, the `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`", and entry must be made in the `risk-log`.

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
        <title>Risk Title</title>
        <description>
            <p>This is a general description of the identified risk.</p>
        </description>
        <statement>
            <p>This is a statement about the identified risk in the context of this
system.</p>
        </statement>
        <status>open</status>

        <characterization>
            <origin>
                <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            </origin>
            <facet name="likelihood" system="https://fedramp.gov/ns/oscal" value="high">
                <prop name="state" value="initial" />
            </facet>
            <facet name="impact" system="https://fedramp.gov/ns/oscal" value="moderate">
                <prop name="state" value="initial" />
            </facet>
        </characterization>
    </risk>

    <finding uuid="951325ce-c0ca-4f8f-9b37-11ccf5258f3b">
        <title>[EXAMPLE]TCW Objective AC-1(a)(1)[1] (Examine)</title>
        <description><p>cut.</p></description>
        <origin><!-- cut --></origin>
        <target type="objective-id" target-id="ac-1.a.1_obj.1">
```



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 `lifecycle` flag on the `response` field must be set to:
  - **`recommendation`**
- The `type` flag on the response `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/reference/datatypes/#markup-multiline

```
            <prop name="implementation-status"
                ns="https://fedramp.gov/ns/oscal" value="implemented"/>
            <status>not-satisfied</status>
        </target>
        <related-observation observation-uuid="d02f9117-84e3-4993-af59-c5ce5e8675ab"/>
        <associated-risk risk-uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9"/>
    </finding>
</result>
```

5.6.1. Test Case Workbook: Recommendation for Mitigation

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

There may be more than one `response` 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 `response` assemblies.

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

If the risk is closed during testing, there must be an additional `response`-assembly with a `lifecycle` value of "`completed`".

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

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

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
        <title>Risk Title</title>
        <description>
            <p>This is a description of the identified risk.</p>
        </description>
        <statement>
            <p>This is a statement about the identified risk.</p>
        </statement>
        <status>open</status>
        <characterization>
            <origin>
                <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            </origin>
            <facet name="likelihood" system="https://fedramp.gov/ns/oscal" value="high">
                <prop name="state" value="initial" />
            </facet>
            <facet name="impact" system="https://fedramp.gov/ns/oscal" value="moderate">
                <prop name="state" value="initial" />
            </facet>
        </characterization>
        <!-- recommendations for risk remediation -->
        <response uuid="fde4758d-6417-4f35-ba71-278af4f008f8"
                  lifecycle="recommendation">
            <title>Remediation Title</title>
            <description>
                <p>A description of the recommended remediation.</p>
                <p>TCW: Assessor's recommended remediation
                   (lifecycle='recommendation').</p>
            </description>
            <origin>
                <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            </origin>
        </response>
        <!-- other recommendations for risk remediation (cut) -->
        <response uuid="scan-tool-recommendation-uuid" lifecycle="recommendation" />
        <response uuid="other-recommendation-uuid" lifecycle="recommendation" />
    </risk>
</result>
```

5.7. Automated Tools

Automated scanning tool output is simply another finding; however, the target 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 collected 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 actor-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 assessment-assets assembly and copied to the SAR. If not, the scanning tool should be added to the SAR results local-definitions/assessment-assets assembly as described in the *Guide to OSCAL-based Security Assessment Plans (SAP), Section 4.13, 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.

[Image intentionally left blank.]

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

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
        <description>
            <p>Undocumented devices found on network.</p>
        </description>
        <method>TEST</method>
        <type>finding</type>
        <origin>
            <actor type="tool" actor-uuid="9d194268-a9d1-4c38-839f-9c4aa57bf71e"></actor>
        </origin>
        <subject type="inventory-item" subject-uuid="f61f4408-2cb8-444a-a312-bc88412e7c61" />
        <subject type="inventory-item" subject-uuid="02075556-3660-4112-8982-02fc7d6fac00" />
        <subject type="inventory-item" subject-uuid="5efe2c07-9fdf-453a-8457-6471046082fb" />
        <subject type="component" subject-uuid="75b059f2-a9ba-40b1-a1e0-881196ca1ead" />
        <relevant-evidence href="#19a07333-4e87-46dc-abab-adad60e706b9">
            <description>
                <p>Raw scanner tool output - discovery scan.</p>
            </description>
        </relevant-evidence>
        <collected>2022-10-10T00:00:00Z</collected>
        <remarks>
            <p>Undocumented hosts are entered into the SAR's local-definitions.</p>
        </remarks>
    </observation>
    <finding uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
        <title>Discovery Scan Results</title>
        <description><p>The results of the discovery scan.</p></description>
        <origin>
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <actor type="party" actor-uuid="e934d8b5-13e5-4f77-b55e-871e6f2df2fe" />
        </origin>
        <related-observation observation-uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d"/>
    </finding>
</result>
```

5.7.1. Automated Tools: Discovery Scans

Any undocumented devices identified by the discovery scans must be added to the SAR's `local-definitions` 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*.

[Image intentionally left blank.]

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

```xml
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <!-- title, description, start, end -->
    <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
        <description>
            <p>Undocumented devices found on network.</p>
        </description>
        <method>TEST</method>
        <type>finding</type>
        <origin>
            <actor type="tool" actor-uuid="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <actor type="party" actor-uuid="e934d8b5-13e5-4f77-b55e-871e6f2df2fe" />
        </origin>
        <subject type="inventory-item" subject-uuid="f61f4408-2cb8-444a-a312-
bc88412e7c61" />
        <subject type="inventory-item" subject-uuid="02075556-3660-4112-8982-
02fc7d6fac00" />
        <subject type="inventory-item" subject-uuid="5efe2c07-9fdf-453a-8457-
6471046082fb" />
        <subject type="component" subject-uuid="75b059f2-a9ba-40b1-a1e0-881196ca1ead" />
        <relevant-evidence href="#19a07333-4e87-46dc-abab-adad60e706b9">
            <description>
                <p>Raw scanner tool output - discovery scan.</p>
            </description>
        </relevant-evidence>
        <collected>2022-10-10T00:00:00Z</collected>
        <remarks>
            <p>Undocumented hosts are entered into the SAR's result/local-definitions
section as inventory-items or components.</p>
            <p>Undocumented hosts are listed in the observations assembly as
subjects.</p>
            <p>The origin must contain the UUID of the tool used to perform the
scan.</p>
        </remarks>
    </observation>

    <finding uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
        <title>Discovery Scan Results</title>
        <description><p>The results of the discovery scan.</p></description>
        <related-observation observation-uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d"/>
    </finding>
</result>
```

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

[Image intentionally left blank.]

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

Automated Tools: Identified Vulnerabilities

There must be one `risk` assembly for each unique vulnerability. All devices identified as having that unique vulnerability must be itemized with `subject` fields in the `observation` assemblies.

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` field. One `subject` 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

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
        <title>Risk Title</title>
        <description>
            <p>This is a description of the identified risk.</p>
            <!-- <p>TCW: Identified Risk.</p> -->
            <p>Scans: Vulnerability Description.</p>
            <!-- <p>Pen Test: Risk Description.</p> -->
            <!-- <p>RET: Description.</p> -->
        </description>

        <statement>
            <p>This is a statement about the identified risk.</p>
            <!-- <p>TCW: Risk Statement..</p> -->
            <p>Scans: N/A.</p>
            <!-- <p>Pen Risk Statement.</p> -->
            <!-- <p>RET: Risk Statement.</p> -->
        </statement>
        <status>open</status>

        <characterization>
            <origin>
                <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            </origin>
            <facet name="likelihood" system="https://fedramp.gov" value="high">
                <prop name="state" value="initial"/>
            </facet>
            <facet name="likelihood" system="https://fedramp.gov" value="moderate">
                <prop name="state" value="initial"/>
            </facet>
        </characterization>

        <response uuid="fde4758d-6417-4f35-ba71-278af4f008f8" lifecycle="recommendation">
            <title>Remediation Title</title>
            <description>
                <p>A description of the recommended remediation.</p>
                <!-- <p>TCW: Assessor's recommended remediation (type='recommendation').</p> -->
                <p>Scans: Tool's recommended remediation (type='recommendation')</p>
```

[Image intentionally left blank.]

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

```
                <!-- <p>Pen Test: Assessor's recommended remediation (type='recommendation')</p> -->
                <!-- <p>RET: Assessor's recommended remediation (type='recommendation').</p> -->
                <!-- <p>POA&amp;M: CSP's intended remediation (no type flag).</p> -->
            </description>
        </response>

    </risk>
</result>
```

See next page for risk assembly

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

FedRAMP required risk-metric data, such as likelihood and impact are specified with `facet` fields with `system` flag 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 initial 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

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <!-- title, description, start, end -->
    <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>
        <statement>
            <p>This is a statement about the identified risk as provided by the tool.</p>
        </statement>
        <status>open</status>

        <characterization>
            <origin>
                <actor type="tool" actor-uuid="040937c3-2e0e-407a-bb3c-d4e61ac1c460" />
            </origin>
            <facet name="vulnerability-id" system="http://csrc.nist.gov/ns/oscal/unknown"
                value="VulID-001" />
            <facet name="plugin-id" system="http://csrc.nist.gov/ns/oscal/unknown"
                value="Plugin-ID" />
            <facet name="iavm-severity" system="https://us-cert.cisa.gov/" value="high" />

            <facet name="vulnerability-id" system="http://cve.mitre.org"
                value="CVE-2020-00000"></facet>
            <facet name="impact" system="http://csrc.nist.gov/ns/oscal/unknown"
                value="high" />
            <facet name="AV" system="http://www.first.org/cvss/v3.1"
                value="network" />
```

[Image intentionally left blank.]

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

            <facet name="likelihood" system="https://fedramp.gov" value="moderate">
                <prop name="state" value="residual"/>
            </facet>
            <facet name="impact" system="https://fedramp.gov" value="moderate">
                <prop name="state" value="residual"/>
            </facet>
        </characterization>

    </risk>
</result>
```

For information about the remediation assembly, see *Section 5.6.1, Test Case Workbook: Recommendation for Mitigation*.

5.8. Penetration Testing: Findings

FedRAMP requires exactly one `finding` assembly for each risk identified through penetration testing. Required reporting, such as spear phishing tests, each must have their own finding assembly as well. Each finding has a `related-observation` referencing observation (where additional details are recorded) via the `uuid` flag. At the end of the `finding` assembly, the UUID for the penetration test lead or team member must be listed as the `actor-uuid` for the finding. Note that there may be more than one penetration test member listed.

The `observation` assembly contains the `method` field which must be set to "`TEST`", and the `type` field which must be set to "`finding`". The `observation` assembly also contains the `collected` field which must be set to the automation tool's discovery timestamp, or the date and time observed. The assessors who gathered the evidence are identified at the bottom of the finding assembly using `actor-uuid` fields.

The `href` flag in the `relevant-evidence` field must contain a URI fragment that points to the `resource` containing the penetration testing report. Section 4.4.3 describes how to reference evidence resources. The back-matter resource containing the penetration test must also have a prop with a name of "`type`" and with a value of " `report`".

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <observation uuid="a38f3bba-5b71-400d-b8f2-d808e1d4627f">
        <description><p>Penetration Testing</p></description>
        <method>TEST</method>
        <type>finding</type>
        <origin>
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
        </origin>
        <related-evidence href="#4739a1e6-b861-4e38-b9b9-7be33d463a5b"><!-- cut -->
        </related-evidence>
        <collected>2022-10-10T00:00:00Z</collected>
    </observation>

    <finding uuid="b56edab1-8cdc-45f9-8589-35f1bd7b3348">
        <title>[EXAMPLE]Penetration Test Result</title>
        <description><p>A finding from penetration testing activities.</p></description>
        <origin>
            <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            <actor type="party" actor-uuid="e934d8b5-13e5-4f77-b55e-871e6f2df2fe" />
        </origin>
        <related-observation observation-uuid="a38f3bba-5b71-400d-b8f2-d808e1d4627f"/>
        <associated-risk risk-uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07"/>
        <remarks>
            <p>If a penetration test result is favorable, such as to say the SOC detected the
activities appropriately, no risk is required.</p>
            <p>If a penetration test result identifies a vulnerability or deficiency, the risk
assembly is required.</p>
        </remarks>
    </finding>

    <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
        <!-- cut -->
    </risk>
</result>
```

[Image intentionally left blank.]

5.9. Penetration Testing: Identified Risks

Some penetration test results may be reportable even if they do not represent a risk. For example, the spear phishing test results must be reported regardless; however, those results only generate a risk if the click rate exceeds a certain threshold. Where a risk must be reported, the risk assembly is added beneath the observation.

For penetration testing, there must be one finding assembly per observation or observation/risk pair.

The risk assembly is populated as described in previous sections.

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

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <!-- observation cut -->

    <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
        <title>Risk Title</title>
        <description>
            <p>This is a description of the issue found by the penetration testing team.</p>
        </description>
        <statement>
            <p>Statement about the risk identified by penetration testing.</p>
        </statement>
        <prop name="priority" ns="https://fedramp.gov/ns/oscal" value="1"/>
        <status>open</status>
        <characterization>
            <origin>
                <actor type="party" actor-uuid="f4568fda-c6d2-4640-adec-0012015af7d0" />
            </origin>
            <facet name="likelihood" system="https://fedramp.gov" value="high">
                <prop name="state" value="initial" />
            </facet>
            <facet name="impact" system="https://fedramp.gov" value="high">
                <prop name="state" value="initial" />
            </facet>
        </characterization>
        <response uuid="69344d05-937e-40f4-9c3f-9aa8702ad99d" lifecycle="recommendation">
            <title>Assessor's Recommendation</title>
            <description>
                <p>A description of the recommended remediation as provided by the
assessor.</p>
            </description>
            <origin>
                <actor type="party" actor-uuid="49f73135-efab-4275-9a79-003656ad890a" />
            </origin>
            <remarks>
                <p>The assessor may add their recommendation.</p>
            </remarks>
        </response>
    </risk>

    <!-- finding cut -->
</result>
```

[Image intentionally left blank.]

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

5.10.Deviations

After risks are identified during an assessment, their status may change. Some are identified as false positive (FP), operationally required (OR), or risk adjusted (RA). As deviations arise, the initial risk information is not modified. Additional content is added to identify these changes. In each case, an additional observation is added to the finding assembly, and additional facet fields are added to the risk assembly. There may be both OR and an RA information in the same finding assembly.

5.10.1. False Positive (FP)

To document a false positive, add a prop to the risk assembly, and change the risk status to "closed". Set the prop name to "false-positive", the ns to "https://fedramp.gov/ns/oscal", and the value to "pending".

Within the observation assembly, provide a description of the false positive. This must have a conformity tag with a value of "false-positive". Typically, the observation method is set to EXAMINE; however, another method may be identified if more appropriate.

Finally, add a separate relevant-evidence assembly for each piece of evidence supporting the FP. Attached evidence, such as screen shots, must be defined as a resource in the back-matter, and cited using a URI fragment (hashtag, followed by the UUID of the resource.)

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <!-- title, description, start, end -->
    <observation uuid="46209140-8263-4e74-b3c9-cead4ffed22c">
        <title>False Positive</title>
        <description><p>False positive justification.</p></description>
        <method>EXAMINE</method>
        <type>false-positive</type>

        <relevant-evidence href="#53af7193-b25d-4ed2-a82f-5954d2d0df61">
            <description>
                <p>A screen shot showing the setting is correct</p></description>
        </relevant-evidence>

        <relevant-evidence href="https://vendor.site/describing/something.htm">
            <description>
                <p>Vendor detail describing why this happens.</p></description>
        </relevant-evidence>
    </observation>

    <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
        <!-- title, description -->
        <prop name="false-positive" ns="https://fedramp.gov/ns/oscal"
            value="pending"/>
        <!-- risk statement -->
        <status>closed</status>
    </risk>
</result>
```

FedRAMP allowed values for false-positive prop:

- investigating
- pending
- approved
- withdrawn

[Image intentionally left blank.]

An operationally required risk is an open risk, which is allowed to remain.
The `status` must remain "`open`". Do <u>not</u> set the `status` to "`closed`".

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

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

5.10.2. Operationally Required (OR)

To document an operationally required risk, add a `prop` to the `risk` assembly, and keep the risk `status` as "`open`". Set the `prop` name to " `operational-requirement` ", the `ns` to "`https://fedramp.gov/ns/oscal`", and the value to "`pending`".

Within the `observation` assembly, provide a justification for the operational requirement. This must have a conformity tag with a value of "`operational-requirement`". Typically, the observation `method` is set to `EXAMINE`; however, another method may be identified if more appropriate.

Finally, add a separate `relevant-evidence` assembly for each piece of evidence supporting the FP. Attached evidence, such as screen shots, must be defined as a `resource` in the `back-matter`, and cited using a URI fragment (hashtag, followed by the UUID of the `resource`.)

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">

    <observation uuid="9de7cba9-40fc-4c4d-b6af-01bd24f1def6">
        <title>Operational Requirement</title>
        <description><p>Justification for the OR.</p></description>
        <method>EXAMINE</method>
        <type>operational-requirement</type>

        <relevant-evidence href="#53af7193-b25d-4ed2-a82f-5954d2d0df61">
            <description>
                <p>Screen shot showing impact when patched.</p>
            </description>
        </relevant-evidence>

        <relevant-evidence
            href="https://vendor.site/article/describing/something.htm">
            <description>
                <p>Vendor detail describing why this happens.</p>
            </description>
        </relevant-evidence>
    </observation>

    <risk uuid="e552fb72-d662-4c01-b2d7-4dcb2086bb07">
        <!-- title, description -->
        <prop name="operational-requirement" ns="https://fedramp.gov/ns/oscal"
            value="pending"/>

        <!-- risk statement -->
        <status>open</status>
    </risk>
</result>
```

FedRAMP allowed values for `operational-requirement` prop:

- `investigating`
- `pending`
- `approved`
- `withdrawn`

[Image intentionally left blank.]

Using the Common Vulnerability Scoring System (CVSS)

When using CVSS scoring to justify a risk adjustment, the CVSS metrics are added as additional risk-metric fields. There must be one risk-metric field for each CVSS metric.

```
<risk-metric name="AV" system="CVSSv3.1">network</risk-metric>
```

See *Appendix A, CVSS Scoring* for more information.

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

5.10.3. Risk Adjustment (RA)

To document an operationally required risk, add a `prop` to the `risk` assembly and keep the risk `status` as "`open`". Set the `prop` name to "`risk-adjustment`", the `ns` to "`https://fedramp.gov/ns/oscal`", and the value to "`pending`".

Within the `observation` assembly, provide a justification for the risk adjustment. This must have a conformity tag with a value of "`risk-adjustment`". Typically, the observation `method` is set to `EXAMINE`; however, another method may be identified if more appropriate.

Use `facet` fields to adjust risk by lowering either likelihood, impact, or both. Within the `facet` fields, set a `prop` with the name “`state`” to indicate whether this is an “`initial`” or “`adjusted`” risk metric.

Finally, `mitigating-factor` assemblies. One describing each mitigating factor. If an SSP implementation statement describes the mitigating factor, link to it using the `implementation-uuid` flag.

Representation

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

    <observation uuid="7acee179-1570-4ea0-94dc-01b8c0a29c0a">
        <title>Risk Adjustment</title>
        <description><p>Justify the risk.</p></description>
        <method>EXAMINE</method>
        <type>risk-adjustment</type>
    </observation>

    <risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
        <prop name="risk-adjustment" ns="https://fedramp.gov/ns/oscal"
            value="pending"/>
        <characterization>
            <origin>
                <actor type="tool" actor-uuid="040937c3-2e0e-407a-bb3c-d4e61ac1c460" />
            </origin>

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

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

FedRAMP allowed values for `risk-adjustment` prop:

- `investigating`
- `pending`
- `approved`
- `withdrawn`

[Image intentionally left blank.]

```
            </facet>
        </characterization>
        <mitigating-factor uuid="fd061039-e9b0-4b4c-a78b-ca024d411174"
            implementation-uuid="46f4c261-e488-4fb5-84d6-6a61dd30c3d7">
            <!-- cut -->
        </mitigating-factor>
        <!-- risk statement -->
        <status>open</status>
    </risk>
</result>
```

5.11.Risk Closure

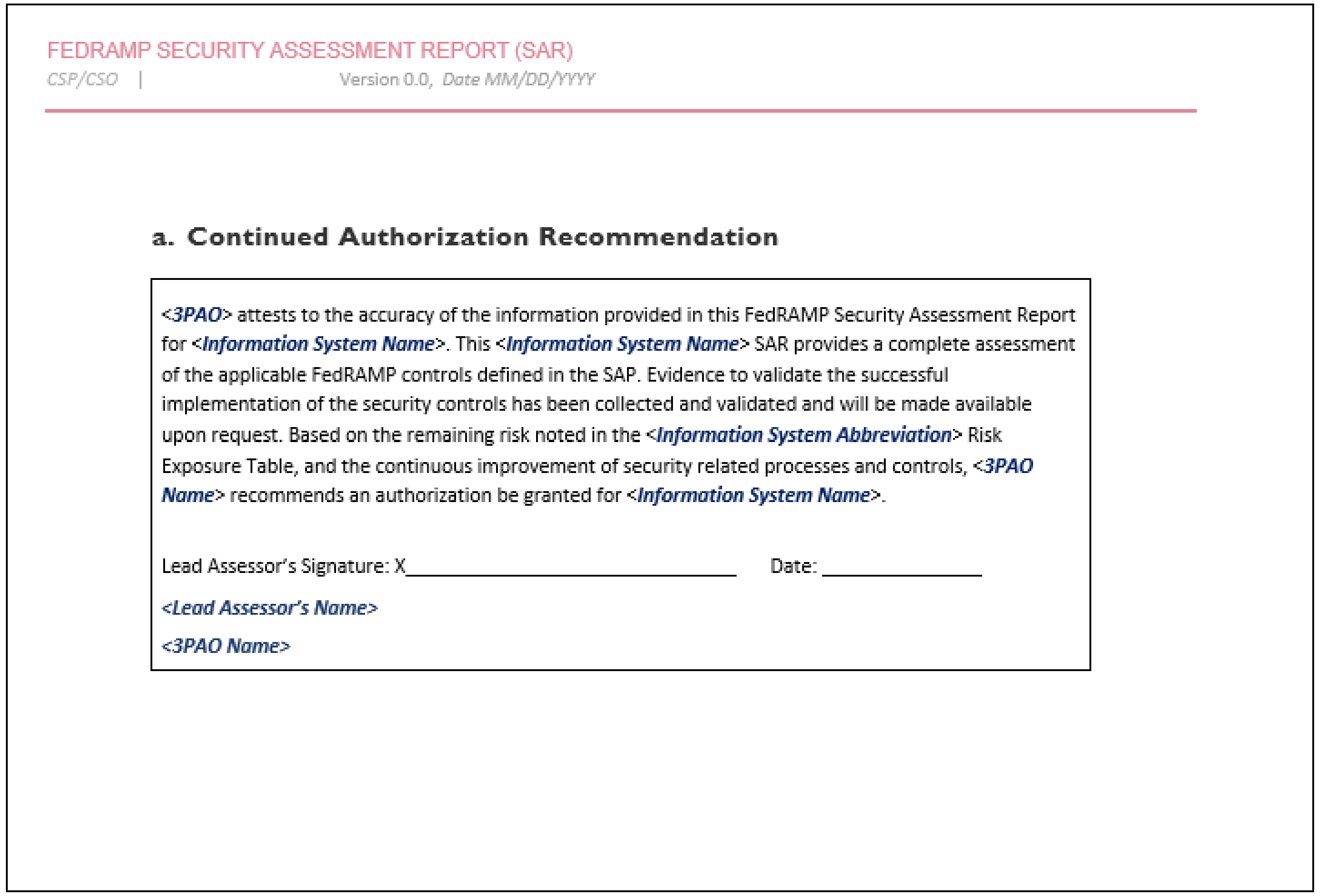
Once identified, risks must remain in the SAR; however, if the CSP closes the risk before testing is complete, it may be marked as closed in the SAR. To represent a risk closure, change the risk `status` to "`closed`", then add an `entry` field and `risk-log` assembly, with a `status-change value` of "`closed` ".

In the `risk-log` , describe the action(s) taken by the CSP to close the risk.

Representation

```
<result uuid="c62765e1-b221-4890-9fb8-93fe84a41c25">
    <risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
        <title>Vulnerability Title</title>
        <description><p>cut</p></description>
        <statement><p>cut</p></statement>
        <status>closed</status>

        <characterization/> <!-- cut for brevity -->

        <response uuid="a3106e23-8b79-4b1b-abf4-74f16c51ad0c"
lifecycle="recommendation">
            <title>Tool's Recommendation</title>
            <description>
                <p>A description of the recommended remediation as provided by the
tool.</p>
            </description>
            <origin>
                <actor type="tool" actor-uuid="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
            </origin>
        </response>
        <response uuid="69344d05-937e-40f4-9c3f-9aa8702ad99d" lifecycle="planned">
            <title>Assessor's Recommendation</title>
            <description>
                <p>A description of the recommended remediation as provided by the
assessor.</p>
            </description>
            <origin>
                <actor type="party" actor-uuid="49f73135-efab-4275-9a79-003656ad890a" />
            </origin>
        </response>

        <risk-log>
            <entry uuid="0b09e341-cf3c-4de7-b728-751c6e88b653">
                <title>Closed</title>
                <description>
                    <p>Describe what action(s) the CSP took to close the risk.</p>
                    <p>Applied patch. Vulnerability no longer found in subsequent
scan.</p>
                </description>
                <start>2022-07-07T00:00:00Z</start>
                <status-change>closed</status-change>
            </entry>
        </risk-log>
    </risk>
</result>
```

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



FEDRAMP SECURITY ASSESSMENT REPORT (SAR)

CSP/CSO | Version 0.0, *Date MM/DD/YYYY*

a. Continued Authorization Recommendation

<*3PAO*> attests to the accuracy of the information provided in this FedRAMP Security Assessment Report for <*Information System Name*>. This <*Information System Name*> SAR provides a complete assessment of the applicable FedRAMP controls defined in the SAP. Evidence to validate the successful implementation of the security controls has been collected and validated and will be made available upon request. Based on the remaining risk noted in the <*Information System Abbreviation*> Risk Exposure Table, and the continuous improvement of security related processes and controls, <*3PAO Name*> recommends an authorization be granted for <*Information System Name*>.

Lead Assessor's Signature: X________________________ Date: ____________

<Lead Assessor's Name>

<3PAO Name>

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

5.12.Continued Authorization Recommendation

There must be a prop field with a value indicating whether the assessor recommends the system for authorization or reauthorization. This must be a FedRAMP extension with the name "`recommend-authorization`". If the recommendation is "`no`" or "`provisionally`", the first paragraph of the Continued Authorization Recommendation should be generated by a SAR tool, as follows:

> *A total of [# of risks] system risks were identified for [system name], including [#high] High risks, [#moderate] Moderate risks, [#low] Low risks, and [#operationally-required] of operationally required risks.*

The "other information as may be required" may be added as a part assembly in the assets section.

Each risk may have a priority value assigned to it. This is another FedRAMP extension prop with the `name` flag set to "`priority`". A priority value of "1" represents the most important risk. "2" represents the second most important risk. Each number should be unique. Do not assign a priority value to a risk that will not be mitigated, such as an operationally required risk.

Representation

```
<result>
  <attestation>
    <responsible-role role-id="assessment-lead"><party-uuid><!-- uuid-of-assessment-lead --></party-uuid></responsible-role>
    <part name="authorization-statements">
      <prop name="recommend-authorization"
        ns="https://fedramp.gov/ns/oscal" value="yes"/>
      <part name="authorization-statement">
        <prop name="sort-id" value="001"/>
        <p>[3PAO] attests to the accuracy of the information provided in this FedRAMP Security Assessment Report for the annual
assessment
            of [Information System Name]</p>
      </part>
      <part name="authorization-statement">
        <prop name="sort-id" value="002"/>
        <p>This [Information System Name] SAR provides a complete assessment of the applicable FedRAMP controls defined
in the SAP.
            Evidence to validate the successful implementation of the security controls has been collected and validated, and will
be made
            available upon request.</p>
      </part>
      <part name="authorization-statement">
        <prop name="sort-id" value="999"/>
        <p>Based on the remaining risk noted in the [Information System Abbreviation] Risk Exposure Table,  and the
continuous improvement
            of security related processes and controls, [3PAO Name] [recommends |does not recommend | provisionally
recommends]
            continued authorization be granted for [Information System Name].</p>
      </part>
    </part>
  </attestation>
  <!-- assessment-activities -->
  <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>
    <statement>
      <p>This is a statement about the identified risk as provided by the tool.</p>
    </statement>
    <prop name="priority" ns="https://fedramp.gov/ns/oscal" value="1"/>
  </risk>
</result>
```

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

6. 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 may be generated from content found elsewhere in this document. This includes the:

- Executive Summary
- Purpose
- Laws, Regulations, Standards, and Guidance
- Scope
- Controls to be Assessed
- System Overview
- Assessment Methodology
- Performed Tests
- Assessment Deviations
- Risk Exposure Table
- Risks Corrected During Testing
- Risks Known for Interconnected Systems
- Scan Results (Infrastructure, Database, Web Application, Container, Other, and Unauthenticated)
  - Inventory of Items Scanned
  - False Positive Report
- Document Results
- Manual Test Results
- Test Case Workbook's System Tab
- Test Case Workbook's Control Summary Tab

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

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

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

https://github.com/GSA/fedramp-automation/tree/master/dist/content/ev5/resources

Appendix A. CVSS Scoring

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

Tools should accept either the upper-case abbreviation or the lower-case name on a field-by-field basis. For example, it should be acceptable to use "`AV`" for access vector, and "`privileges-required`" for privileges required, provided both have a `system` value of "http://www.first.org/cvss/v3.1".

All CVSS metrics must be in the same CVSS version, as identified by the `system` flag, for successful computation. Tool developers should ensure the tool performs CVSS calculations as defined by the Forum of Incident Response and Security Teams (FIRST) at https://www.first.org/cvss/.

Representation

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

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

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

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

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