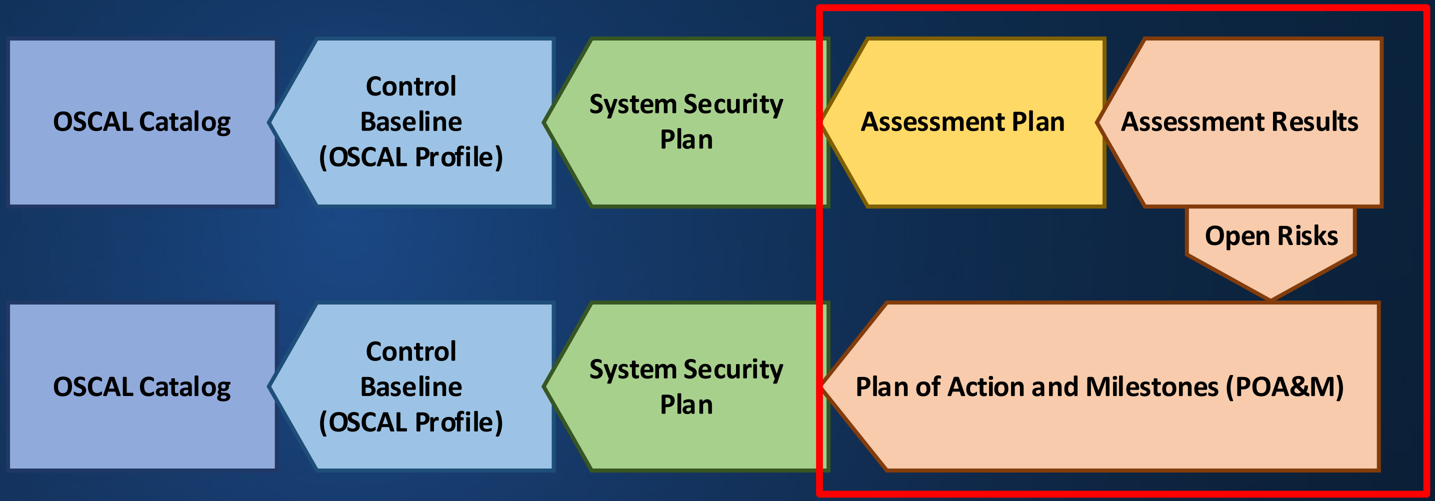
OSCAL Assessment Layers

Assessment Plan, Assessment Results, and POA&M Models

National Institute of Standards and Technology
U.S. Department of Commerce

OSCAL Assessment Models



Reworked from Milestone 3

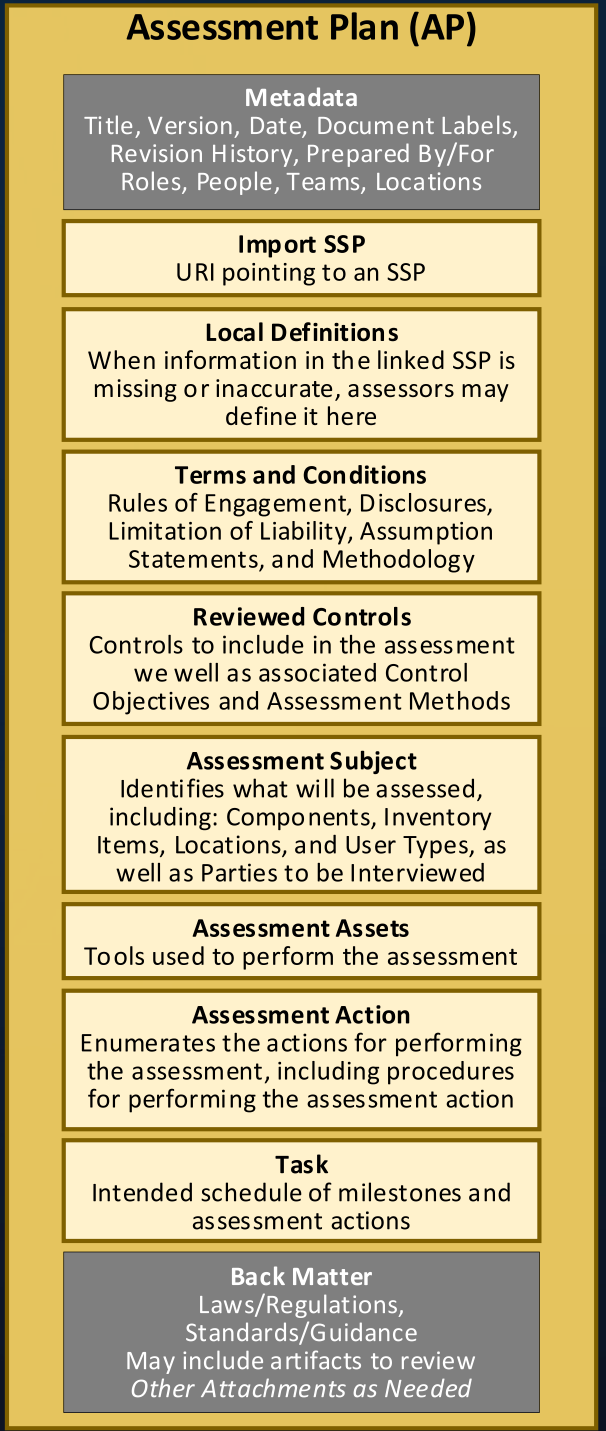
- Greater syntax consistency across OSCAL models
- More emphasis on continuous assessment
- More flexibility for different assessment approaches
- Added syntax in support of assessment templates
- Risk Metrics are now Characterizations and Facets

All Assessment Models are designed to be used

- In the context of a system (via a linked OSCAL SSP)
- In the context of a control baseline (via the SSP's linked OSCAL Profile)

OSCAL Assessment Plan (AP) Model

- **Import SSP:** Identifies the OSCAL SSP
- **Local Definitions:** Missing or incorrect SSP or Profile information
- **Terms and Conditions:** Legal statements, disclaimers, and methodologies
- **Reviewed Controls:** In-scope controls, control objectives, and methods
- **Assessment Subject:** In-scope system elements to be assessed
- **Assessment Assets:** tools and platforms used to perform the assessment
- **Assessment Action:** which *activity* to perform on which *assessment subjects* by which *role* based on what timing?
- **Task**: Assessment schedule with milestones



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

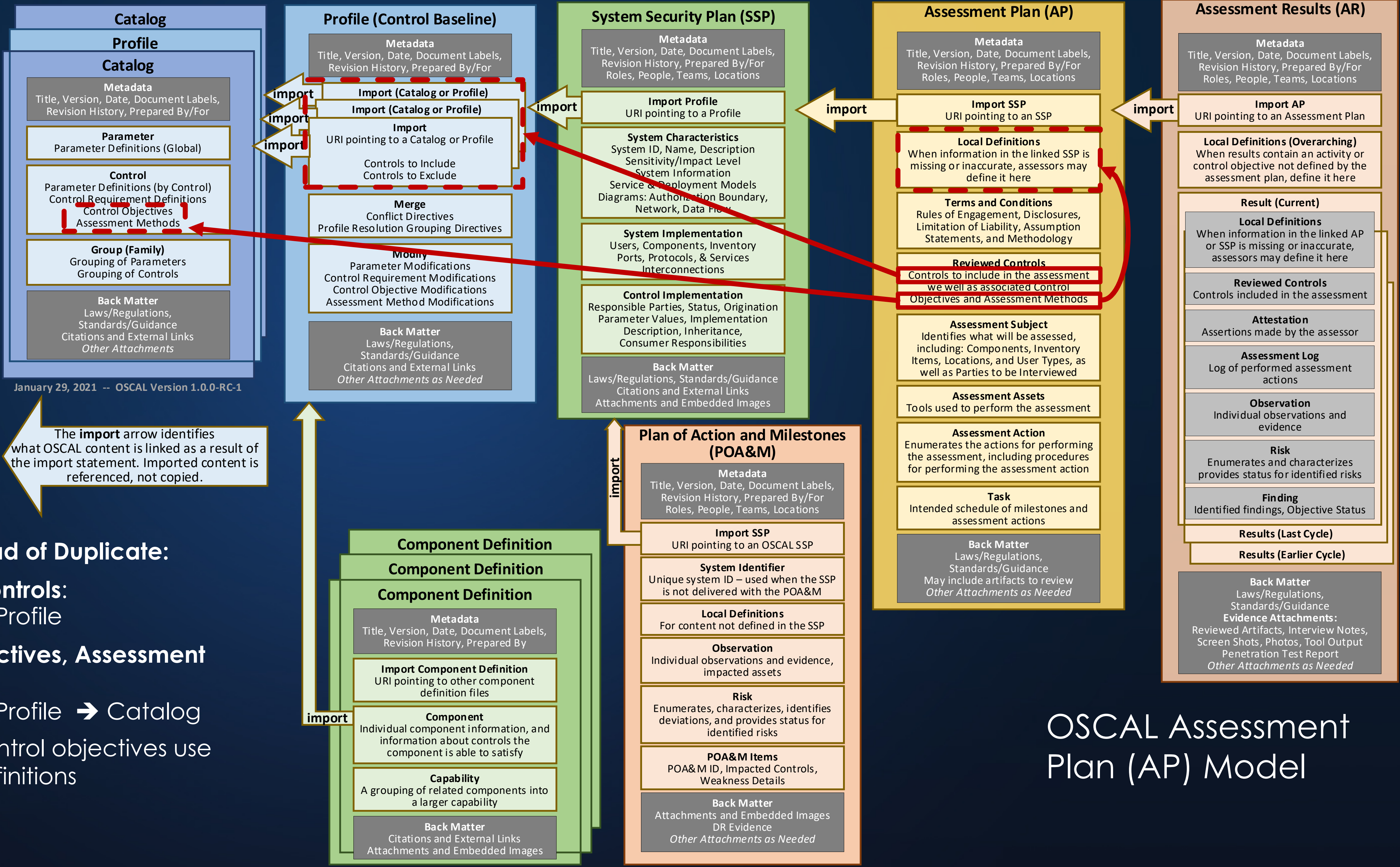
Assessment Assets
Tools used to perform the assessment

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed

OSCAL Assessment Plan (AP) Model



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

System Security Plan (SSP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance,
Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed

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

Plan of Action and Milestones (POA&M)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

Component Definition

Component Definition

Component Definition

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

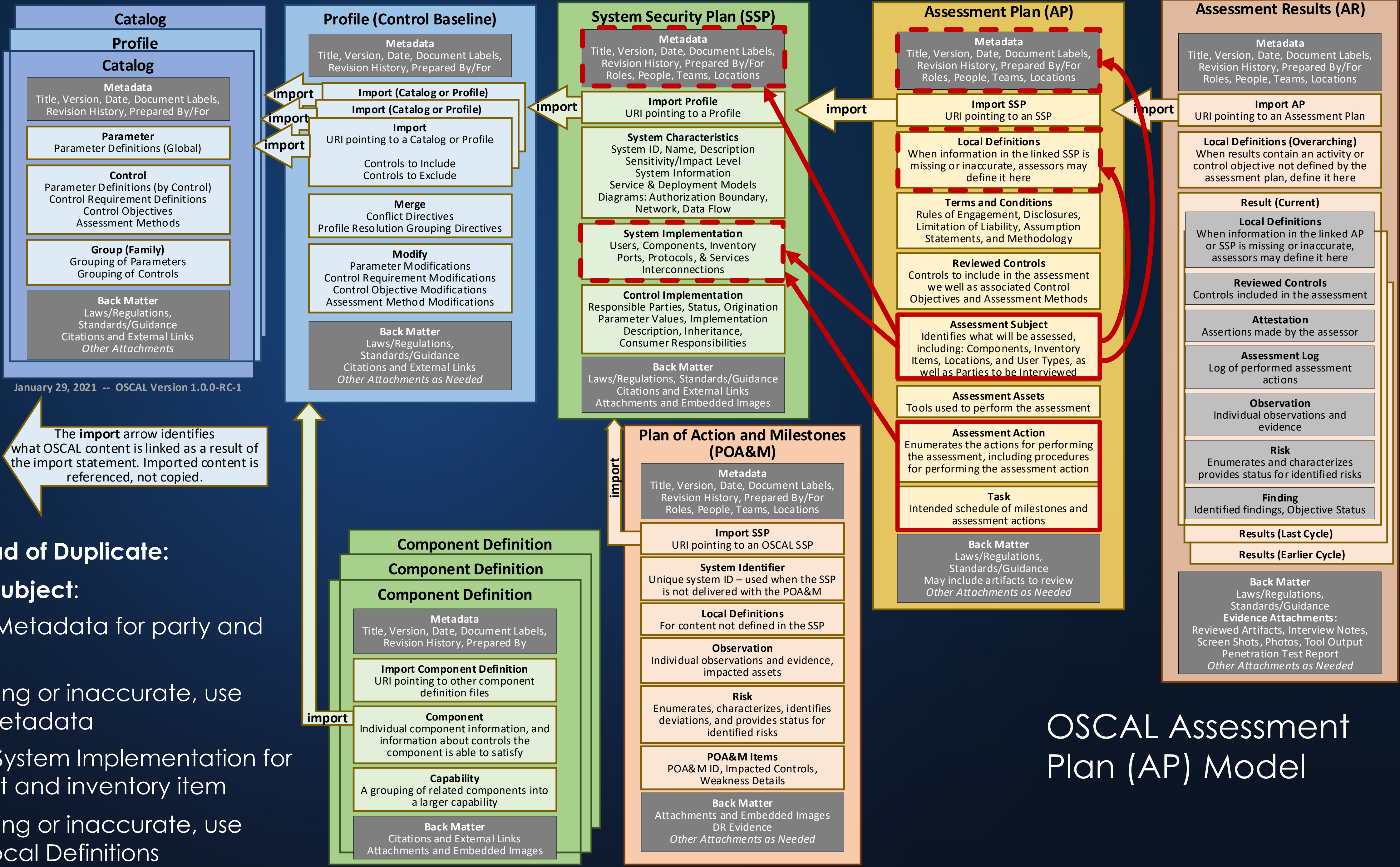
Component
Individual component information, and information about controls the component is able to satisfy

Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images

Reference instead of Duplicate:

- **Reviewed Controls**:
  AP ➔ SSP ➔ Profile
- **Control Objectives, Assessment Methods**
  AP ➔ SSP ➔ Profile ➔ Catalog
- If tailoring control objectives use AP: Local Definitions



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

import

import

import

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

System Security Plan (SSP)

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance, Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

Assessment Plan (AP)

import

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed

Assessment Results (AR)

import

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

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

Plan of Action and Milestones (POA&M)

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

Component Definition

Component Definition

Component Definition

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

Component
Individual component information, and information about controls the component is able to satisfy

Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images

Reference instead of Duplicate:

- **Assessment Subject**:
  - AP ➔ SSP: Metadata for party and location
    - If missing or inaccurate, use AP: Metadata
  - AP ➔ SSP: System Implementation for component and inventory item
    - If missing or inaccurate, use AP: Local Definitions

OSCAL Assessment Plan (AP) Model

OSCAL Assessment Plan (AP) Model Actions, Activities, and Tasks

Assessment Plan (AP) Activities, Actions & Tasks

Local Definitions

Activity

Identifies an assessment activity, including the steps to perform the activity.

Assessment Action

Identifies an *activity* to be performed on specific subjects by specific assessors using specific assessment assets.

Task

Identifies the schedule and/or sequencing for *assessment actions*, as well as assessment milestones

Assessment Plan (AP) Activities, Actions & Tasks EXAMPLE

Local Definitions

Activity: Discovery Scan
Step: identify subnet to scan
Step: etc.

Activity: Authenticated Scan
Step: identify assets to scan
Step: etc.

Assessment Action: Scan Subnets A & B
Activity: Discovery Scan
Activity: Authenticated Scan

Assessment Action: Scan Subnets C & D
Activity: Discovery Scan
Activity: Authenticated Scan

Task: Notify SOC – Start of Scanning
Start/End: March 1, 2021

Task: Network Scanning
Start: March 1, 2021 **End**: March 3, 2020
Related-Action: Scan Subnets A & B
Related-Action: Scan Subnets C & D

Task: Notify SOC – End of Scanning
Start/End: March 3, 2020

Assessment Action
title: Scan Subnets A & B
description: Discovery and Detailed Scan of Primary Data Center

assessment-subject:
include-subject: Location UUID of Primary Data Center
include-subject: Component UUID of Subnet A
include-subject: Component UUID of Subnet B

associated-activity: Discovery Scan
associated-activity: Authenticated Scan

responsible-role: assessment-team

Assessment Action
title: Scan Subnets C & D
description: Discovery and Detailed Scan of Alternat Data Center

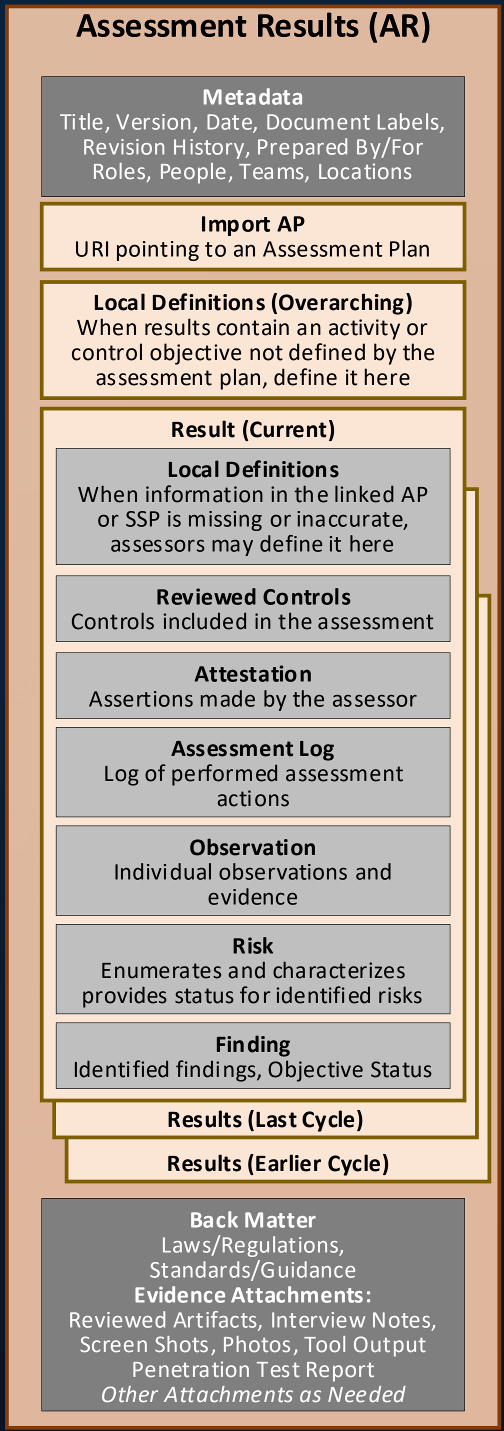
assessment-subject:
include-subject: Location UUID of Alternate Data Center
include-subject: Component UUID of Subnet C
include-subject: Component UUID of Subnet D

associated-activity: Discovery Scan
associated-activity: Authenticated Scan

responsible-role: assessment-team

OSCAL Assessment Results (AR) Model

- **Import AP:** Identifies the OSCAL AP
- **Local Definitions:** When AP information is missing or incorrect
- **Result**: A set of assessment results
  - **Local Definitions:** When SSP or Profile information is missing or incorrect
  - **Reviewed Controls:** Controls actually reviewed
    AR ➔ AP ➔ SSP ➔ Profile
  - **Attestation:** Any overall statements the assessor asserts
  - **Assessment Log:** Who did what, when?
    Activities, Actions, Task: AR ➔ AP
  - **Observation:** A citation of evidence collected
    Assessor, Asset AR: ➔ AP Assessment Subject: AR ➔ AP ➔ SSP
    - **Origin/Actor**: Who or what generated the observation
  - **Risk**: An identified risk (as supported by unfavorable observations)
    - **Characterization/Facet**: Initial and Residual Risk values, CVSS, etc.
  - **Finding**: A conclusion of control satisfaction as supported by observations



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

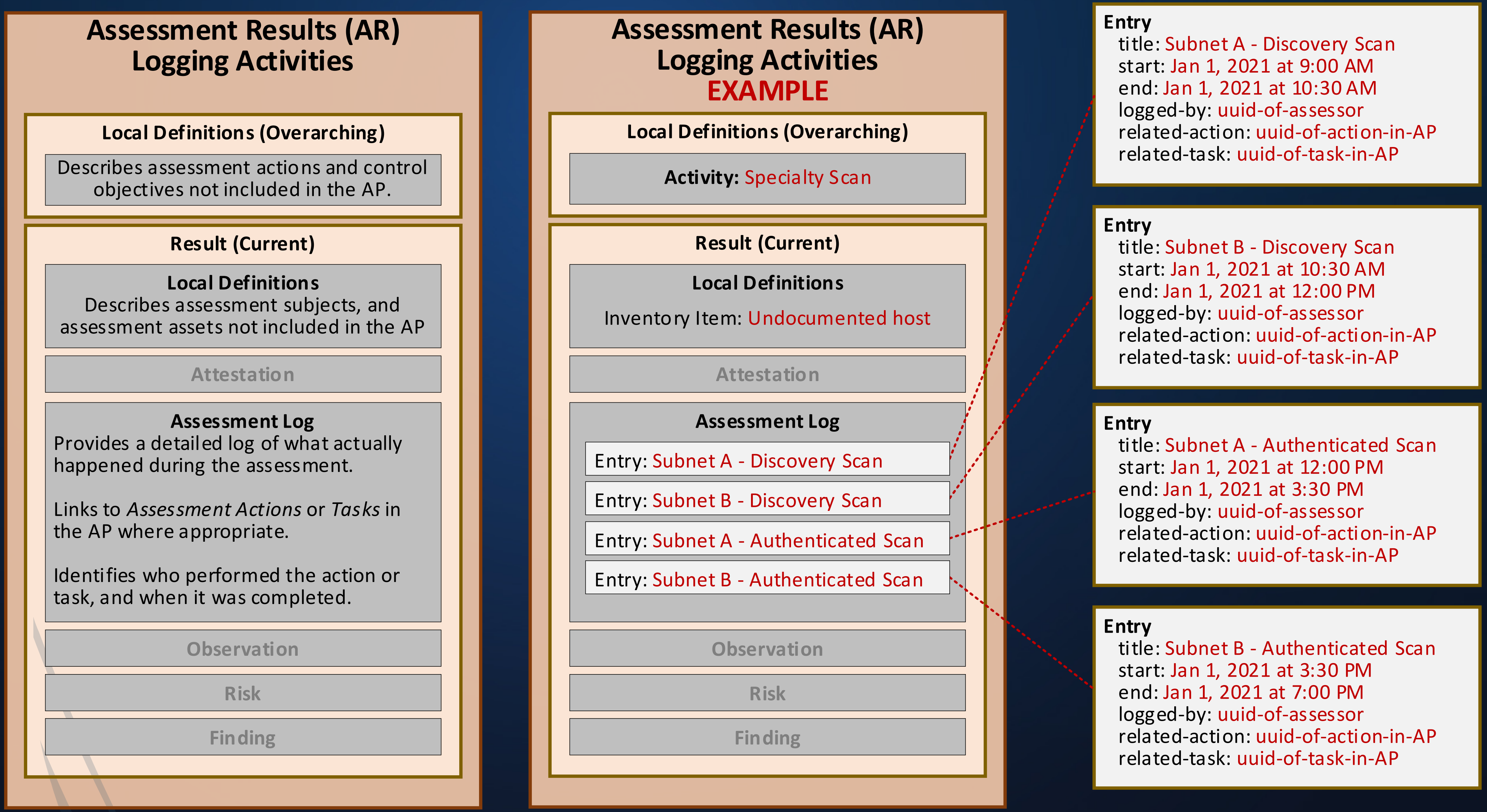
Finding
Identified findings, Objective Status

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

OSCAL Assessment Results (AP) Model Activities and Log Items



Assessment Results (AR) Logging Activities

Local Definitions (Overarching)

Describes assessment actions and control objectives not included in the AP.

Result (Current)

Local Definitions
Describes assessment subjects, and assessment assets not included in the AP

Attestation

Assessment Log
Provides a detailed log of what actually happened during the assessment.

Links to *Assessment Actions* or *Tasks* in the AP where appropriate.

Identifies who performed the action or task, and when it was completed.

Observation

Risk

Finding

Assessment Results (AR) Logging Activities EXAMPLE

Local Definitions (Overarching)

Activity: Specialty Scan

Result (Current)

Local Definitions

Inventory Item: Undocumented host

Attestation

Assessment Log

Entry: Subnet A - Discovery Scan

Entry: Subnet B - Discovery Scan

Entry: Subnet A - Authenticated Scan

Entry: Subnet B - Authenticated Scan

Observation

Risk

Finding

Entry
title: Subnet A - Discovery Scan
start: Jan 1, 2021 at 9:00 AM
end: Jan 1, 2021 at 10:30 AM
logged-by: uuid-of-assessor
related-action: uuid-of-action-in-AP
related-task: uuid-of-task-in-AP

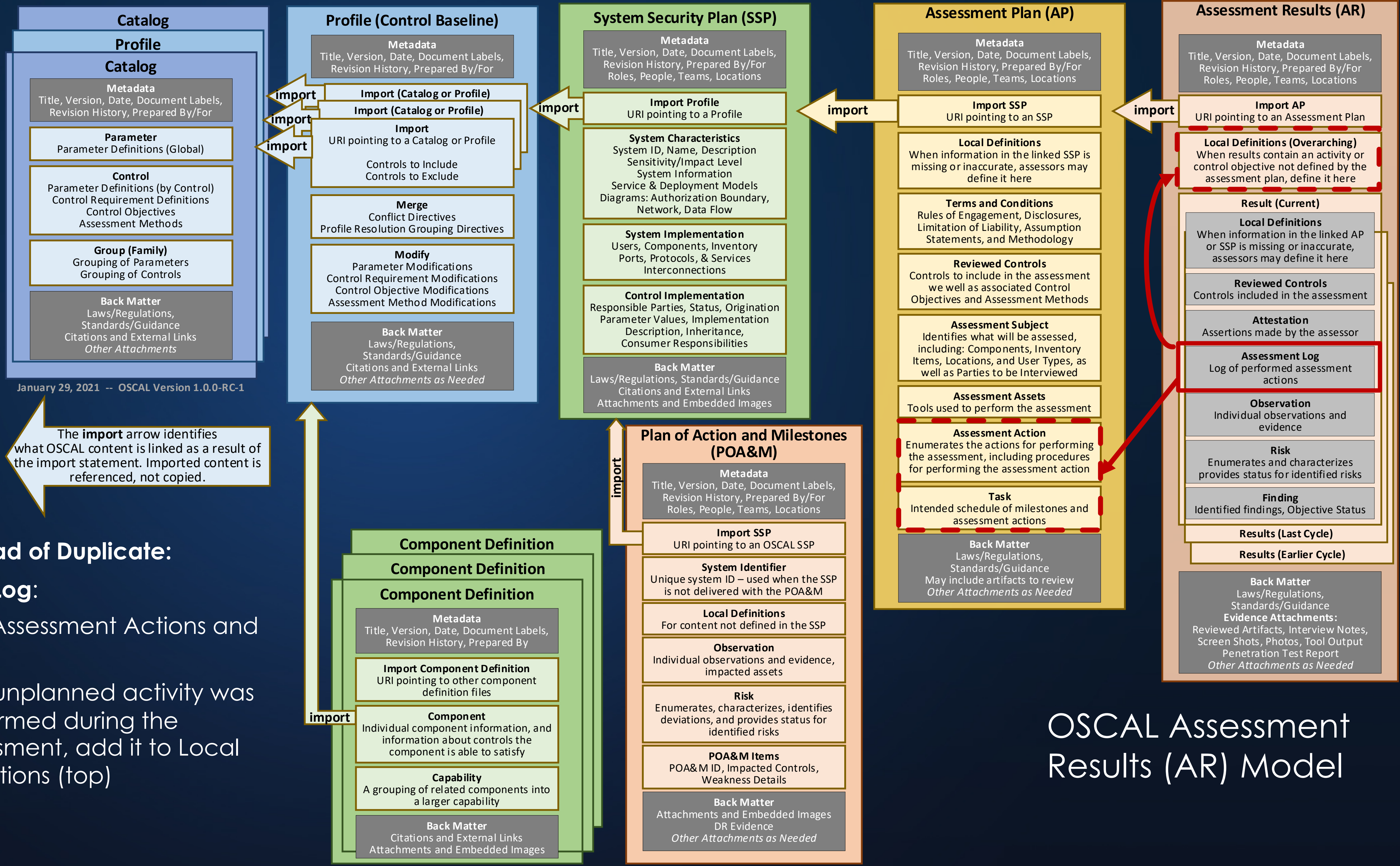
Entry
title: Subnet B - Discovery Scan
start: Jan 1, 2021 at 10:30 AM
end: Jan 1, 2021 at 12:00 PM
logged-by: uuid-of-assessor
related-action: uuid-of-action-in-AP
related-task: uuid-of-task-in-AP

Entry
title: Subnet A - Authenticated Scan
start: Jan 1, 2021 at 12:00 PM
end: Jan 1, 2021 at 3:30 PM
logged-by: uuid-of-assessor
related-action: uuid-of-action-in-AP
related-task: uuid-of-task-in-AP

Entry
title: Subnet B - Authenticated Scan
start: Jan 1, 2021 at 3:30 PM
end: Jan 1, 2021 at 7:00 PM
logged-by: uuid-of-assessor
related-action: uuid-of-action-in-AP
related-task: uuid-of-task-in-AP

Identifies:

- What assessment action or activity was performed
- When
- Who made the log entry



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

import

import

import

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

import

System Security Plan (SSP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance,
Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

import

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

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

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

import

Plan of Action and Milestones (POA&M)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

import

Component Definition

Component Definition

Component Definition

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

Component
Individual component information, and information about controls the component is able to satisfy

Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images

Reference instead of Duplicate:

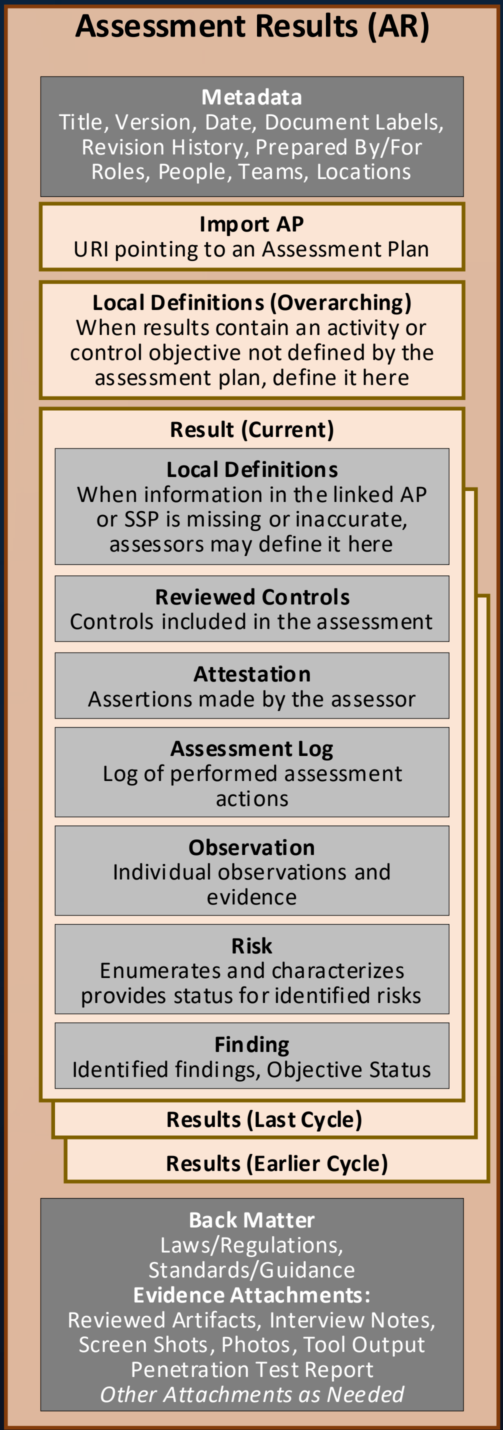
- ➢ **Assessment Log**:
  - ➢ AR ➔ AP: Assessment Actions and Tasks
    - ➢ If an unplanned activity was performed during the assessment, add it to Local Definitions (top)

OSCAL Assessment Results (AR) Model

OSCAL Assessment Results (AR) Model: Finding Scenario 1

Scenario: An inspection confirms that a control is satisfied (Positive Finding)

- **Result:**
  - **Observation (UUID Value):**
    - Origin/Actor: The assessor who performed the inspection
    - Subject: Host 1
    - Collected: Date/time of inspection
    - Relevant Evidence: Link to screen shot
  - **Finding (UUID Value)**
    - **Objective Status**: Control or Control Objective
      - **Status**: Satisfied
    - **Related Observation**: UUID of observation above



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

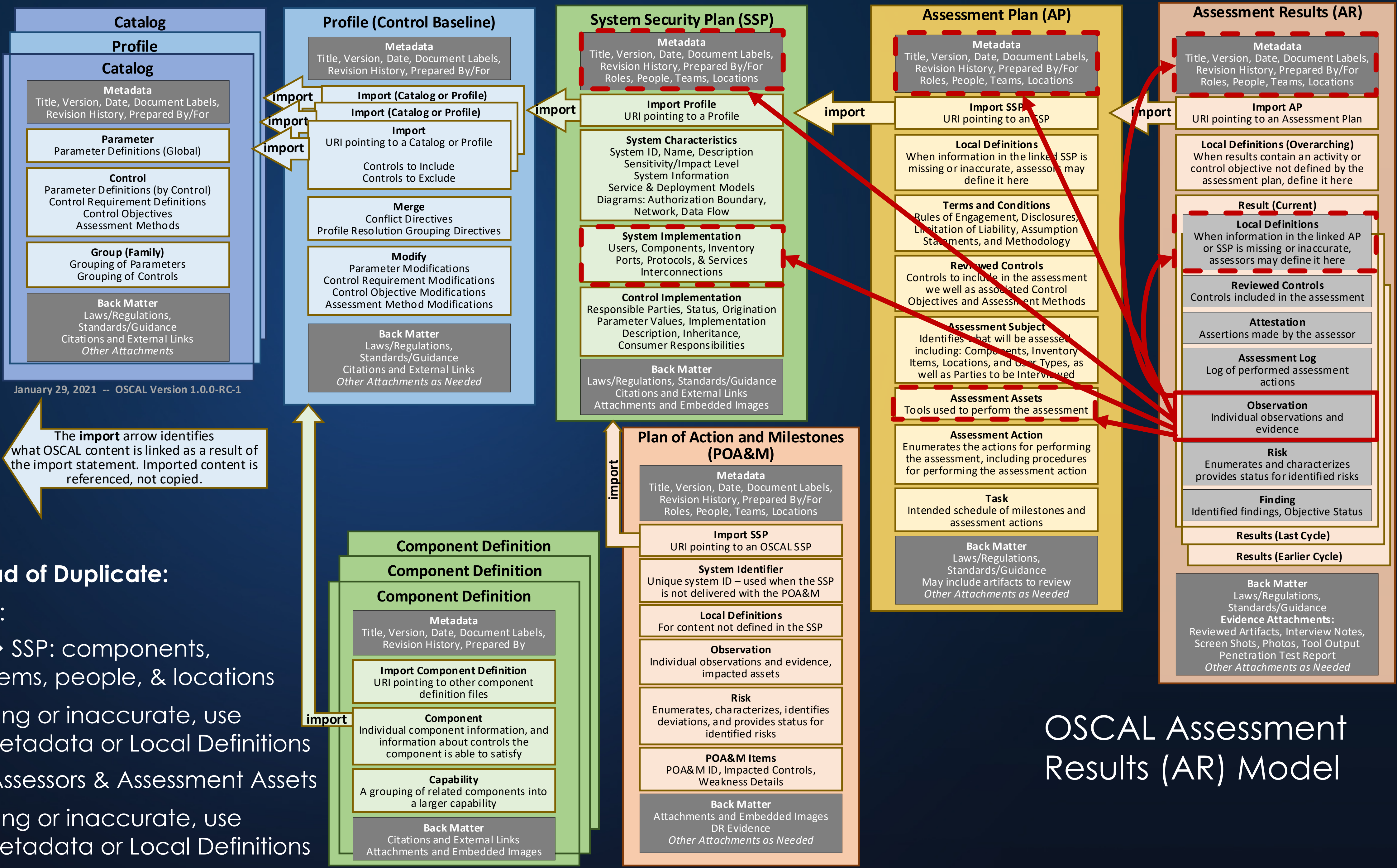
Risk
Enumerates and characterizes provides status for identified risks

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



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

import

import

import

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

System Security Plan (SSP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

import

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance,
Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

Assessment Plan (AP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

import

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed

Assessment Results (AR)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

import

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

Plan of Action and Milestones (POA&M)

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

Component Definition

Component Definition

Component Definition

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

Component
Individual component information, and information about controls the component is able to satisfy

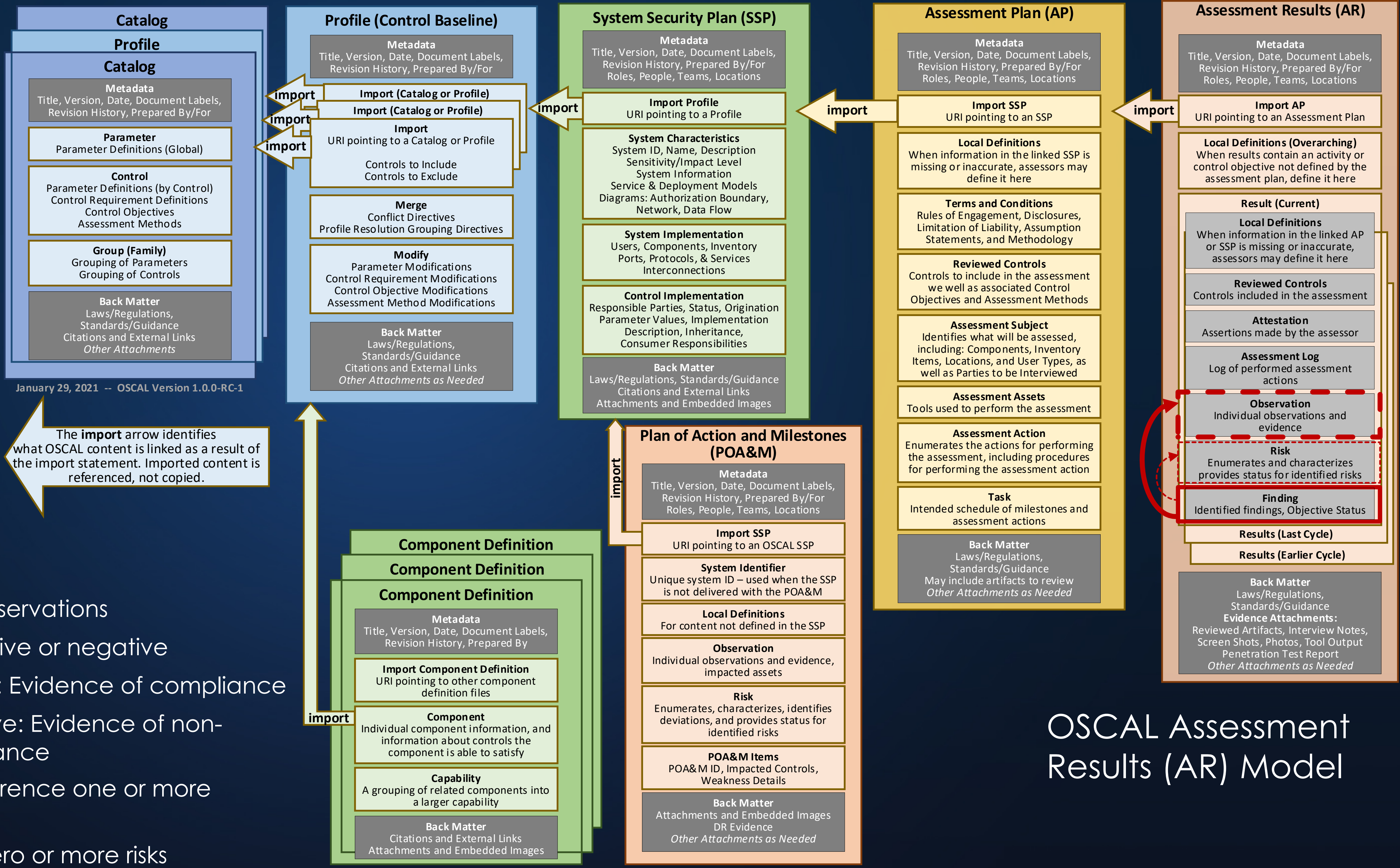
Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images

Reference instead of Duplicate:

- **Observations**:
  - AR ➔ AP ➔ SSP: components, inventory items, people, & locations
    - If missing or inaccurate, use AR: Metadata or Local Definitions
  - AR ➔ AP: Assessors & Assessment Assets
    - If missing or inaccurate, use AR: Metadata or Local Definitions

OSCAL Assessment Results (AR) Model



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

import

import

import

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

System Security Plan (SSP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance, Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

import

Component Definition

Component Definition

Component Definition

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

Component
Individual component information, and information about controls the component is able to satisfy

Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images

import

Plan of Action and Milestones (POA&M)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

import

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

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)

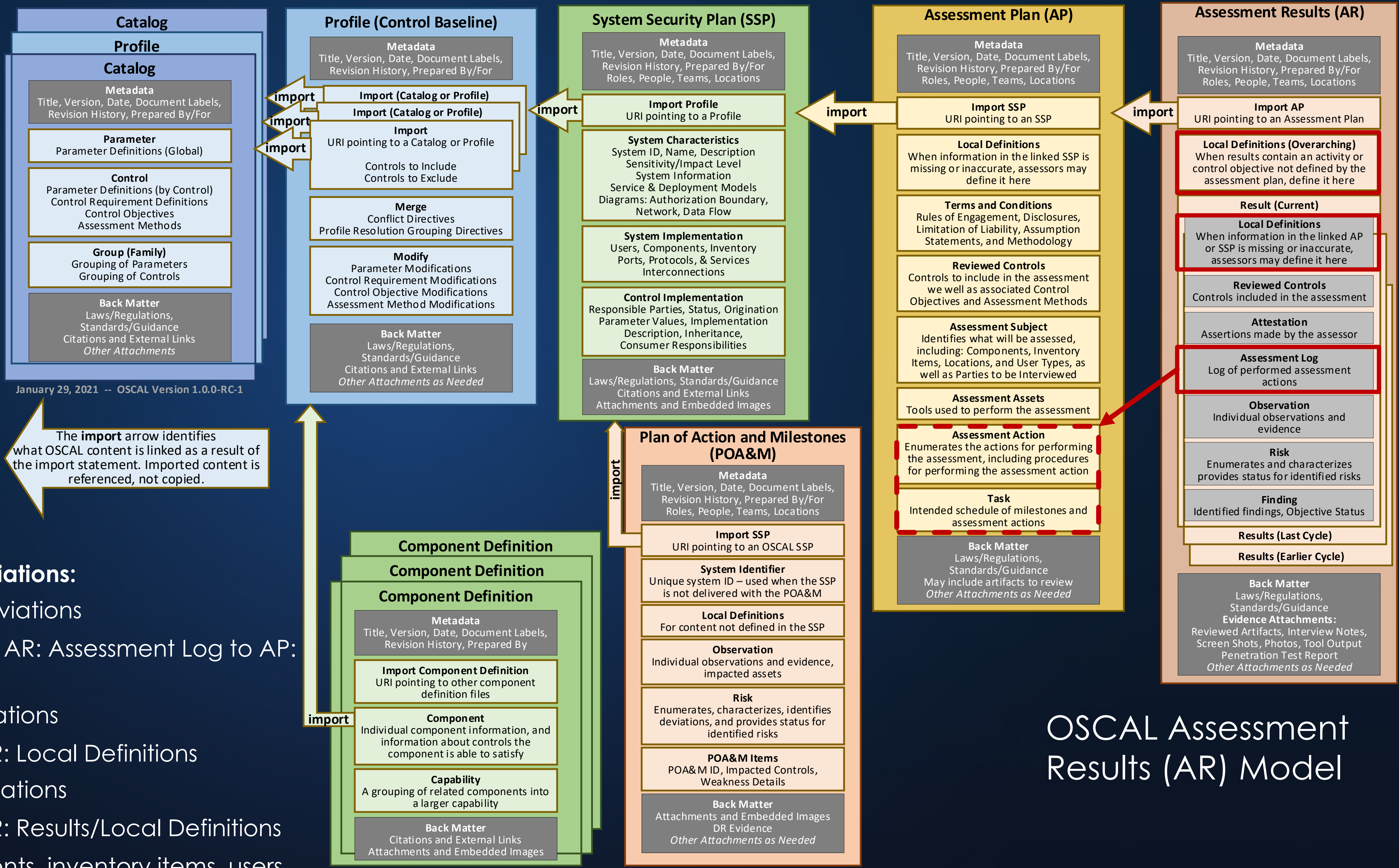
Back Matter
Laws/Regulations, Standards/Guidance
Evidence Attachments:
Reviewed Artifacts, Interview Notes, Screen Shots, Photos, Tool Output
Penetration Test Report
Other Attachments as Needed

Findings:

- Tie risks to observations
- May be positive or negative
  - Positive: Evidence of compliance
  - Negative: Evidence of non-compliance
- *Typically* reference one or more observations
- Reference zero or more risks

OSCAL Assessment Results (AR) Model

OSCAL Assessment Results (AR) Model



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

System Security Plan (SSP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance,
Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed

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

Plan of Action and Milestones (POA&M)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

Component Definition

Component Definition

Component Definition

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

Component
Individual component information, and information about controls the component is able to satisfy

Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

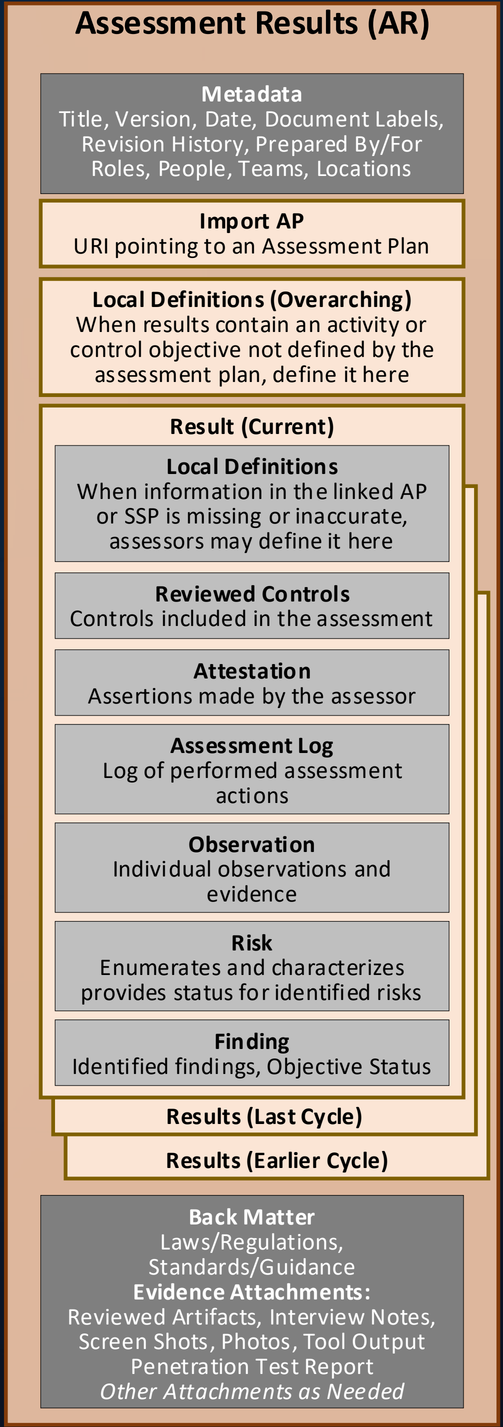
Assessment Deviations:

- Schedule Deviations
  - Compare AR: Assessment Log to AP: Tasks
- Activity Deviations
  - Look in AR: Local Definitions
- All other deviations
  - Look in AR: Results/Local Definitions
  - Components, inventory items, users

OSCAL Assessment Results (AR) Model: Finding Scenario 2

Scenario: Authenticated scan on subnet A finds the same vulnerability on two Linux hosts (Negative Finding)

- **Result:**
  - **Observation (UUID Value):**
    - **Origin/Actor**: The scanning tool
    - **Origin/Actor**: The person operating the tool
    - **Collected**: Date/Time Stamp from Scan
    - **Subject**: Linux Host 1
    - **Subject**: Linux Host 2
    - **Relevant Evidence**: Link to raw scanner tool output file
  - **Risk (UUID Value)**
  - **Finding (UUID Value)**



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)

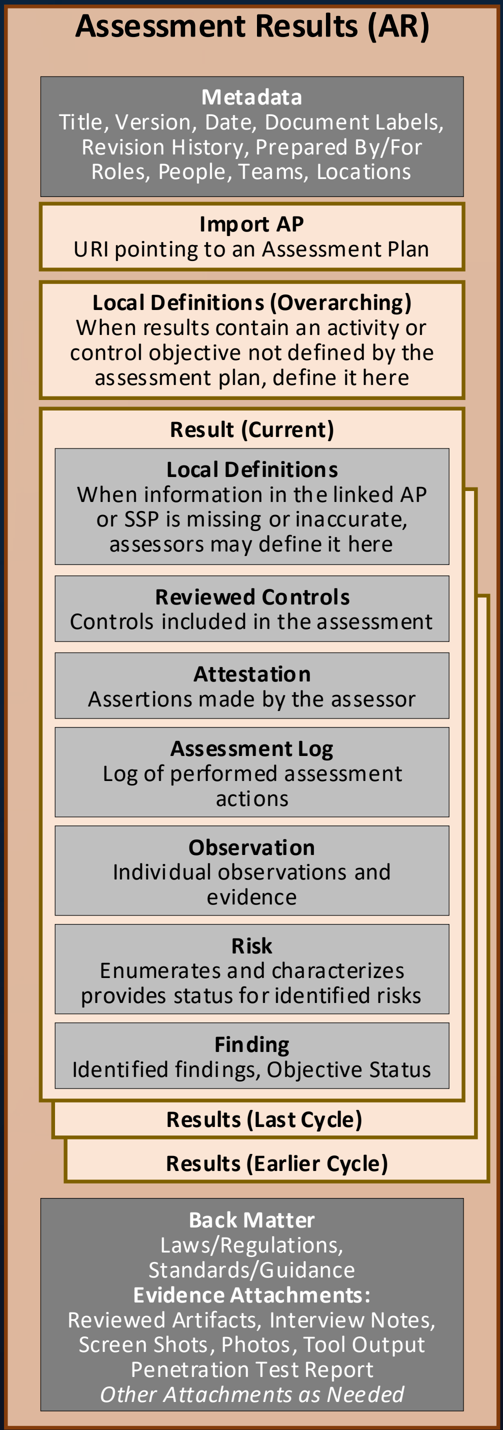
Results (Earlier Cycle)

Back Matter
Laws/Regulations, Standards/Guidance
Evidence Attachments:
Reviewed Artifacts, Interview Notes, Screen Shots, Photos, Tool Output
Penetration Test Report
Other Attachments as Needed

OSCAL Assessment Results (AR) Model: Finding Scenario 2 (continued)

Scenario: Authenticated scan on subnet A finds the same vulnerability on two Linux hosts (Negative Finding)

- **Result**:
  - **Observation (UUID Value)**
  - **Risk (UUID Value):**
    - **Status**: Open
    - **Characterization**
      - **Facet**: Likelihood = moderate
      - **Facet**: Impact = high
      - **Origin**: UUID of scanner tool
  - **Finding (UUID Value)**:
    - **Related Observation**: UUID of Observation
    - **Associated Risk**: UUID of Risk



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

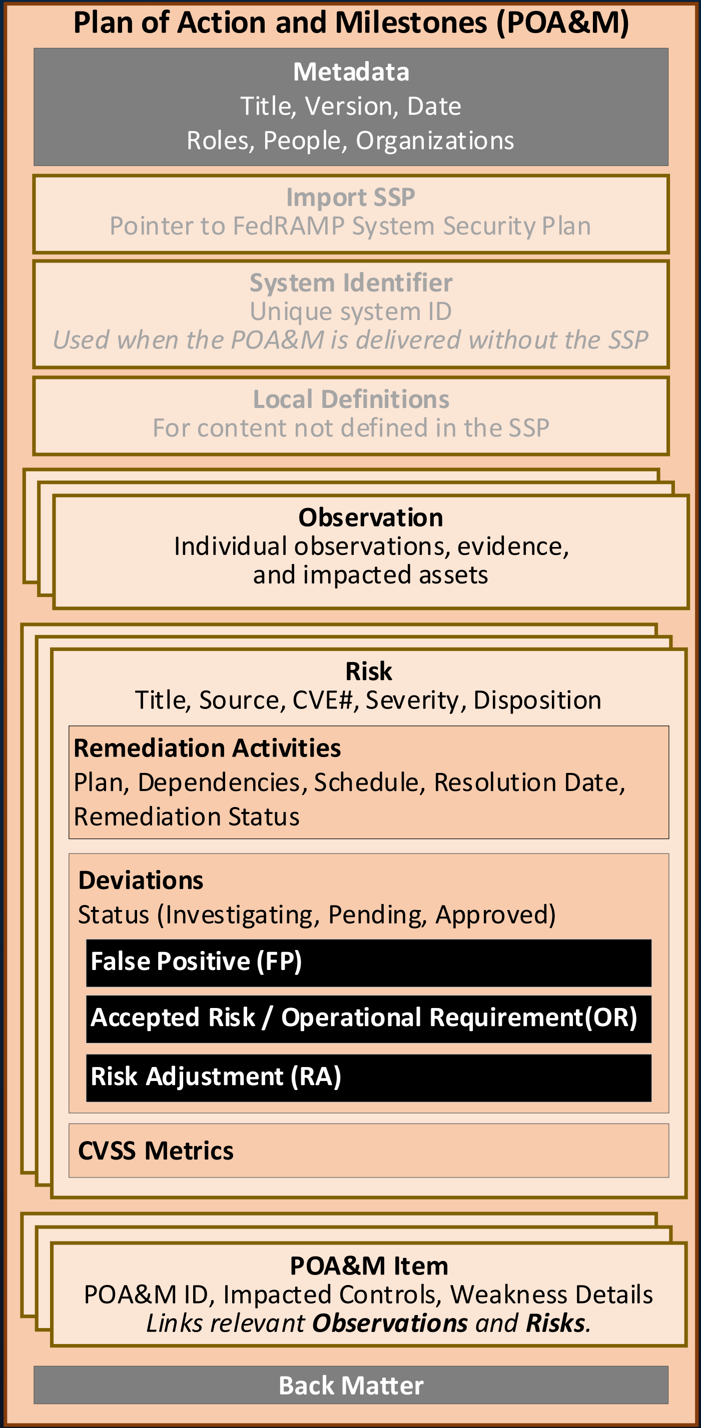
Results (Last Cycle)

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

OSCAL Plan of Action and Milestones (POA&M) Model

- **Import SSP:** Identifies the OSCAL SSP
- **System Identifier**: When POA&M is delivered without an SSP
- **Local Definitions:** When SSP information is missing or incorrect
- **Observation:** A citation of evidence collected
  Subject: POA&M ➔ SSP
- **Risk**: An identified risk (as supported by unfavorable observations) and associated remediation activities
  - **Remediation Activities**: Plans and activities to resolve the risk
  - **Deviations**: Identify and track changes to the risk finding itself
- **POA&M Items**: POA&M entries, each linking risks, observations, and impacted controls



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

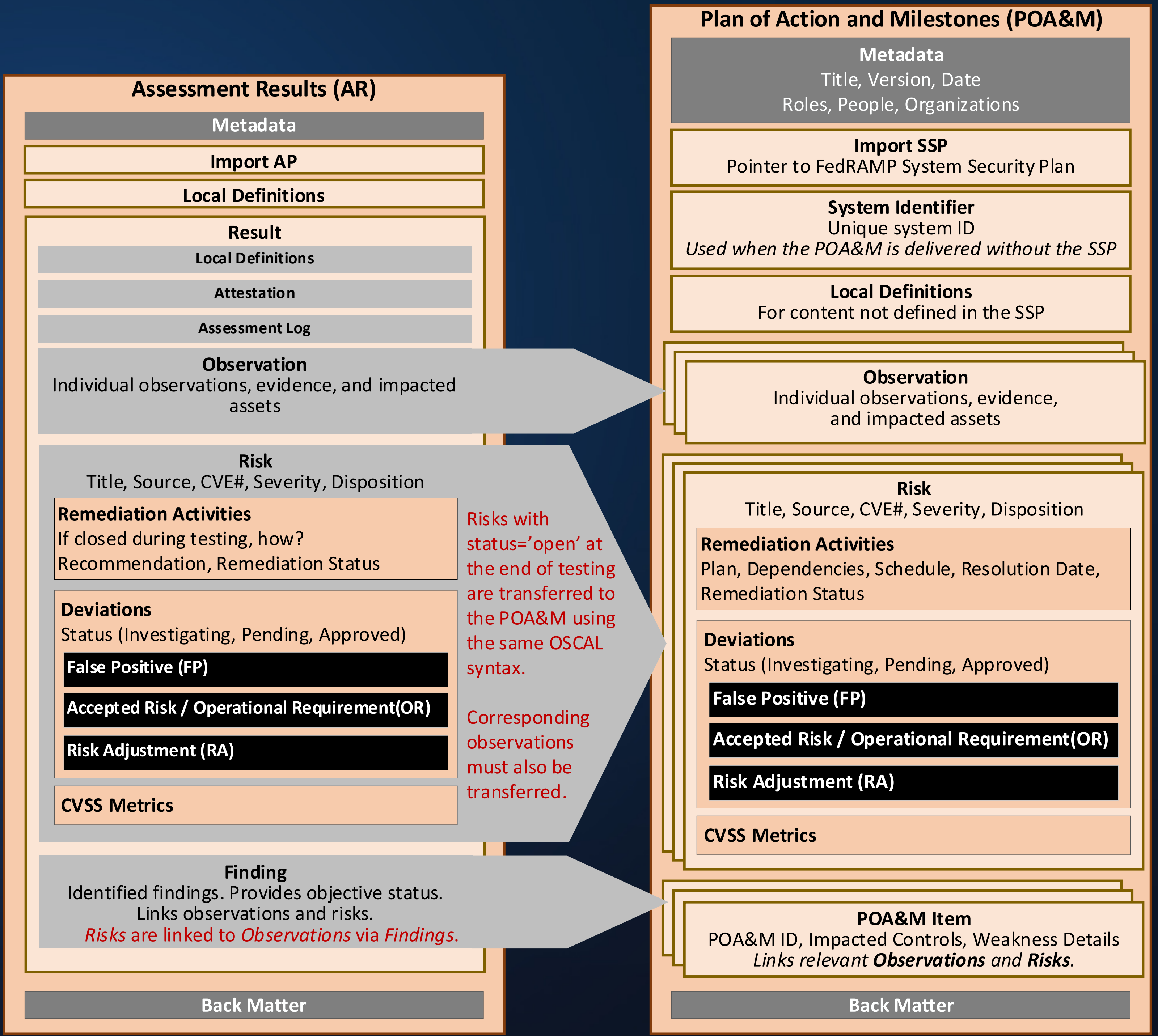
OSCAL AR to POA&M

At the end of an assessment:

- Copy all "open" risks from AR to POA&M
- For every risk, also copy all related observations
- Risks are linked to observations in the Finding

It may also be necessary to copy content from the AP or AR into the POA&M's Local Definitions.

- Typically to ensure Observation/Origin references remain valid
- Example: A scanner tool defined in AP: Assessment Assets



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)

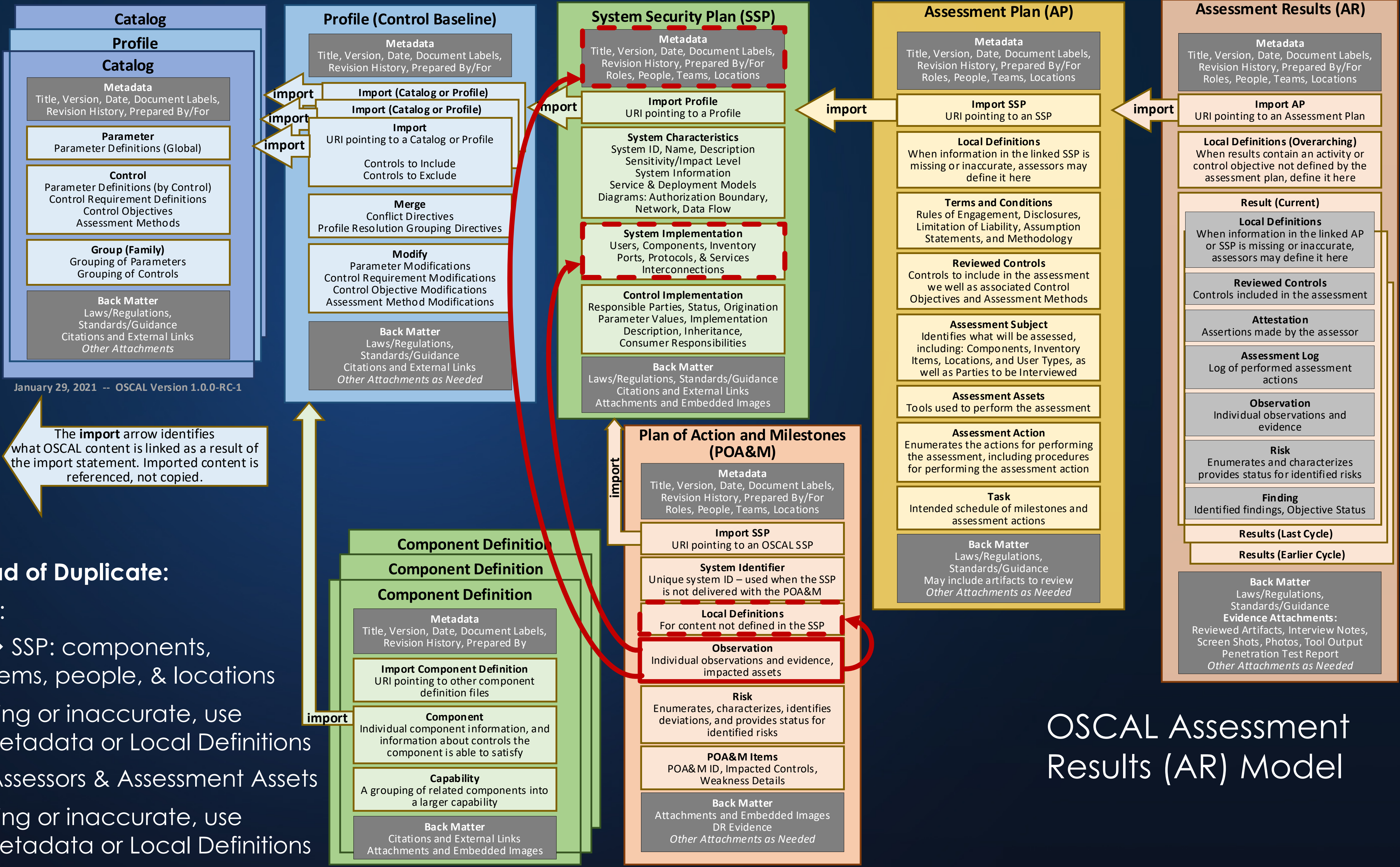
Risk Adjustment (RA)

CVSS Metrics

POA&M Item
POA&M ID, Impacted Controls, Weakness Details
*Links relevant **Observations** and **Risks**.*

Back Matter

OSCAL Assessment Results (AR) Model



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

import

import

import

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

System Security Plan (SSP)

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance, Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

Assessment Plan (AP)

import

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed

Assessment Results (AR)

import

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

Plan of Action and Milestones (POA&M)

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

Component Definition

Component Definition

Component Definition

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

Component
Individual component information, and information about controls the component is able to satisfy

Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images

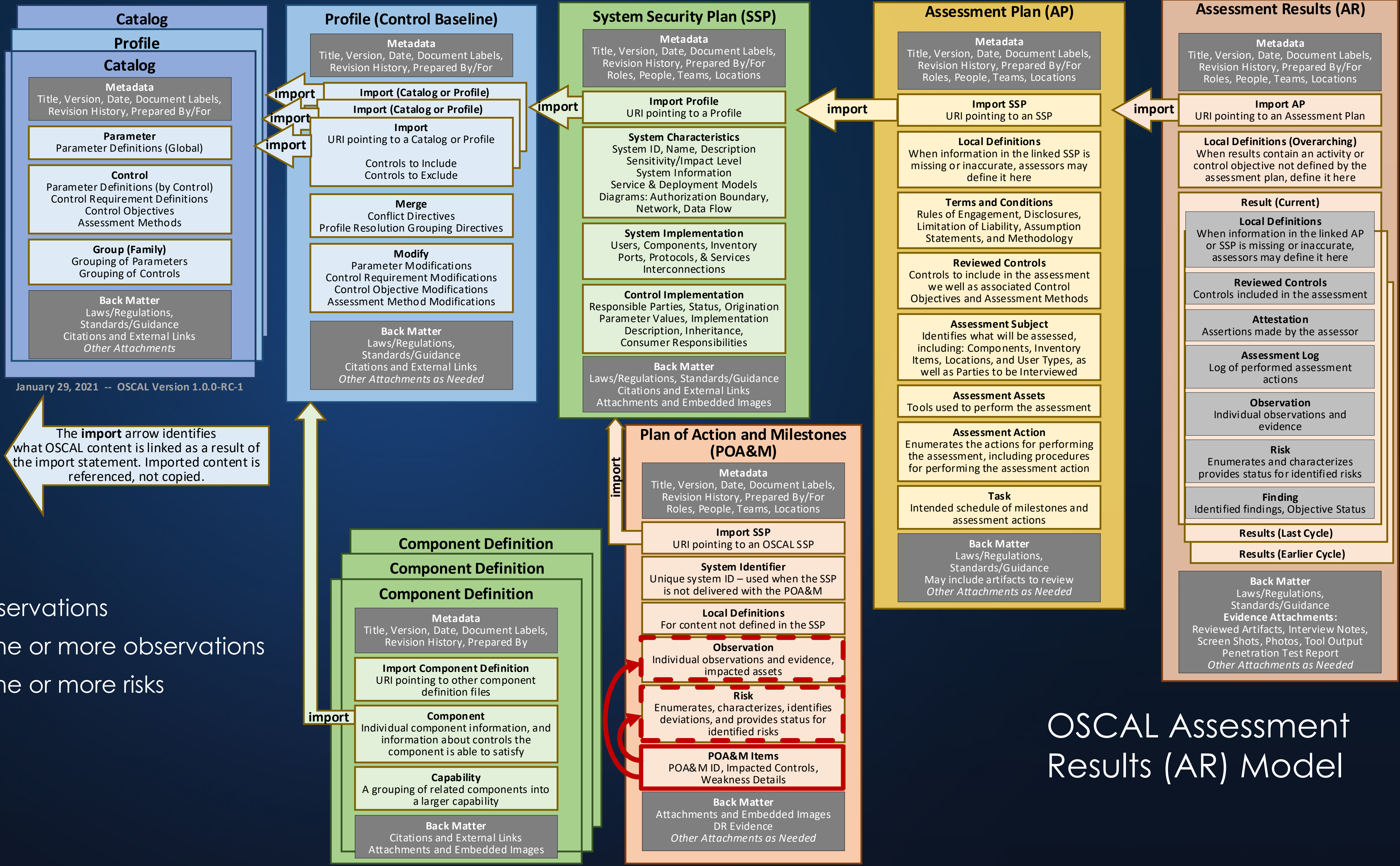
Reference instead of Duplicate:

- **Observations**:
  - AR ➔ AP ➔ SSP: components, inventory items, people, & locations
    - If missing or inaccurate, use AR: Metadata or Local Definitions
  - AR ➔ AP: Assessors & Assessment Assets
    - If missing or inaccurate, use AR: Metadata or Local Definitions

OSCAL Assessment Results (AR) Model

POA&M Items:

- Tie risks to observations
- Reference one or more observations
- Reference one or more risks



Catalog

Profile

Catalog

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Parameter
Parameter Definitions (Global)

Control
Parameter Definitions (by Control)
Control Requirement Definitions
Control Objectives
Assessment Methods

Group (Family)
Grouping of Parameters
Grouping of Controls

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments as Needed

System Security Plan (SSP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance,
Consumer Responsibilities

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Attachments and Embedded Images

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

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

Back Matter
Laws/Regulations, Standards/Guidance
May include artifacts to review
Other Attachments as Needed

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

The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content is referenced, not copied.

Plan of Action and Milestones (POA&M)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

Component Definition

Component Definition

Component Definition

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By

Import Component Definition
URI pointing to other component definition files

Component
Individual component information, and information about controls the component is able to satisfy

Capability
A grouping of related components into a larger capability

Back Matter
Citations and External Links
Attachments and Embedded Images