OSCAL Assessment Layers
Assessment Plan, Assessment Results, and POA&M Models
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
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

**OSCAL Assessment Plan (AP) Model**

**Plan of Action and Milestones (POA&M)**
- Metadata: Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations
- Import Action Plan URI pointing to an OSCAL SSP

**Assessment Plan (AP)**
- Metadata: Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations
- Import Plan of Action and Milestones URI pointing to an SSP

**Assessment Results (AR)**
- Metadata: Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations
- Import Assessment Plan URI pointing to an Assessment Plan

**OSCAL Version 1.0.0**

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.
**Assessment Plan (AP) Model**

**Activities, Actions, and Tasks**

**Local Definitions**

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

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

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

---

**Assessment Action**

**title:** Scan Subnets C & D

**description:** Discovery and Detailed Scan of Alternate Data Center

**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
- Authenticated Scan

**responsible-role:** assessment-team

---

**Assessment Action**

**title:** Scan Subnets A & B

**description:** Discovery and Detailed Scan of Primary Data Center

**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
- Authenticated Scan

**responsible-role:** assessment-team

---

**Assessment Action**

**title:** Scan Subnets A & B

**description:** Discovery and Detailed Scan of Primary Data Center

**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
- Authenticated Scan

**responsible-role:** assessment-team

---

**Assessment Action**

**title:** Scan Subnets C & D

**description:** Discovery and Detailed Scan of Alternate Data Center

**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
- 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
  - **Attestation**: Any overall statements the assessor asserts
  - **Assessment Log**: Who did what, when?
  - **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
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)
Describes assessment subjects, and assessment assets not included in the AP.

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.

Local Definitions (Overarching)

CSV Table:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Title</th>
<th>Start Date</th>
<th>End Date</th>
<th>Logged By</th>
<th>Related Action</th>
<th>Related Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td>Subnet A - Discovery Scan</td>
<td>Jan 1, 2021 at 9:00 AM</td>
<td>Jan 1, 2021 at 10:30 AM</td>
<td>uuid-of-assessor</td>
<td>uuid-of-action-in-AP</td>
<td>uuid-of-task-in-AP</td>
</tr>
<tr>
<td>Entry</td>
<td>Subnet B - Discovery Scan</td>
<td>Jan 1, 2021 at 10:30 AM</td>
<td>Jan 1, 2021 at 12:00 PM</td>
<td>uuid-of-assessor</td>
<td>uuid-of-action-in-AP</td>
<td>uuid-of-task-in-AP</td>
</tr>
<tr>
<td>Entry</td>
<td>Subnet A - Authenticated Scan</td>
<td>Jan 1, 2021 at 12:00 PM</td>
<td>Jan 1, 2021 at 3:30 PM</td>
<td>uuid-of-assessor</td>
<td>uuid-of-action-in-AP</td>
<td>uuid-of-task-in-AP</td>
</tr>
<tr>
<td>Entry</td>
<td>Subnet B - Authenticated Scan</td>
<td>Jan 1, 2021 at 3:30 PM</td>
<td>Jan 1, 2021 at 7:00 PM</td>
<td>uuid-of-assessor</td>
<td>uuid-of-action-in-AP</td>
<td>uuid-of-task-in-AP</td>
</tr>
</tbody>
</table>

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

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

### System Security Plan (SSP)
- Metadata
  - Title, Version, Date, Document Labels, Revision History, Prepared By/For
  - Roles, Teams, Locations

### Plan of Action and Milestones (POA&M)
- Metadata
  - Title, Version, Date, Document Labels, Revision History, Prepared By/For
  - Roles, Teams, Locations

### Assessment Plan (AP)
- Metadata
  - Title, Version, Date, Document Labels, Revision History, Prepared By/For
  - Roles, Teams, Locations

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

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

OSCAL Assessment Results (AR) Model

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

**Import**
- Import AP URI pointing to an Assessment Plan

**Local Definitions**
- When information in the linked AP or SSP is missing or inaccurate, assessors may define it here

**Revised Controls**
- Controls to include in the assessment

**Assessment Plan (AP)**
- Title, Version, Date, Document Labels
- Revision History, Prepared By

**Import**
- Import AP URI pointing to an SSP

**System Security Plan (SSP)**
- Title, Version, Date, Document Labels
- Revision History, Prepared By

**Import**
- Import Catalog (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

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

**Merge**
- Profile Resolution Grouping Directives

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

**Profile (Control Baseline)**
- Title, Version, Date, Document Labels
- Revision History, Prepared By

**Import**
- Import Catalog (Profile)

**Profile**
- URI pointing to a Catalog or Profile

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

**Capability**
- A grouping of related components into a larger capability

**Observation**
- Individual observations and evidence, impacted assets

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

**Back Matter**
- Laws/Regulations, Standards/Guidance
- Evidence Attachments, Reviewed Artifacts, Interview Notes, Screen Shots, Photos, Tool Output

**Plan of Action and Milestones (POA&M)**
- Title, Version, Date, Document Labels
- Revision History, Prepared By

**Import**
- Import Catalog (Profile)

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

**Component Definition**
- Title, Version, Date, Document Labels
- Revision History, Prepared By

**Import**
- Component Definition URI pointing to another component definition file

**Capability**
- A grouping of related components into a larger capability

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

**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

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

**Import SSP**
- URI pointing to an OSCAL SSP

**Parameters**
- System Characteristics
- System Identification
- Policies, Rules, People, Teams

**Profile Resolution Grouping Directives**
- Responsible Parties, Status, Origination Parameter Values, Implementation Descriptions, Inheritance, Consumer Responsibilities

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

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

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

**Assessment Actions**
- Enumerates the actions for performing the assessment, including procedures for performing the assessment action

**Tasks**
- Intended schedule of milestones and assessment actions

**Results**
- Results (Last Cycle)
- Results (Earlier Cycle)

**References**
- **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

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

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

<table>
<thead>
<tr>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import AP</td>
</tr>
</tbody>
</table>

**Local Definitions**

<table>
<thead>
<tr>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual observations, evidence, and impacted assets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title, Source, CVE#, Severity, Disposition</td>
</tr>
</tbody>
</table>

**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.*

---

**Plan of Action and Milestones (POA&M)**

<table>
<thead>
<tr>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title, Version, Date</td>
</tr>
<tr>
<td>Roles, People, Organizations</td>
</tr>
</tbody>
</table>

**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.*
POA&M Items:
- Tie risks to observations
- Reference one or more observations
- Reference one or more risks

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