Open Security Controls Assessment Language
The Anatomy of OSCAL Models
- Assessment Layer -

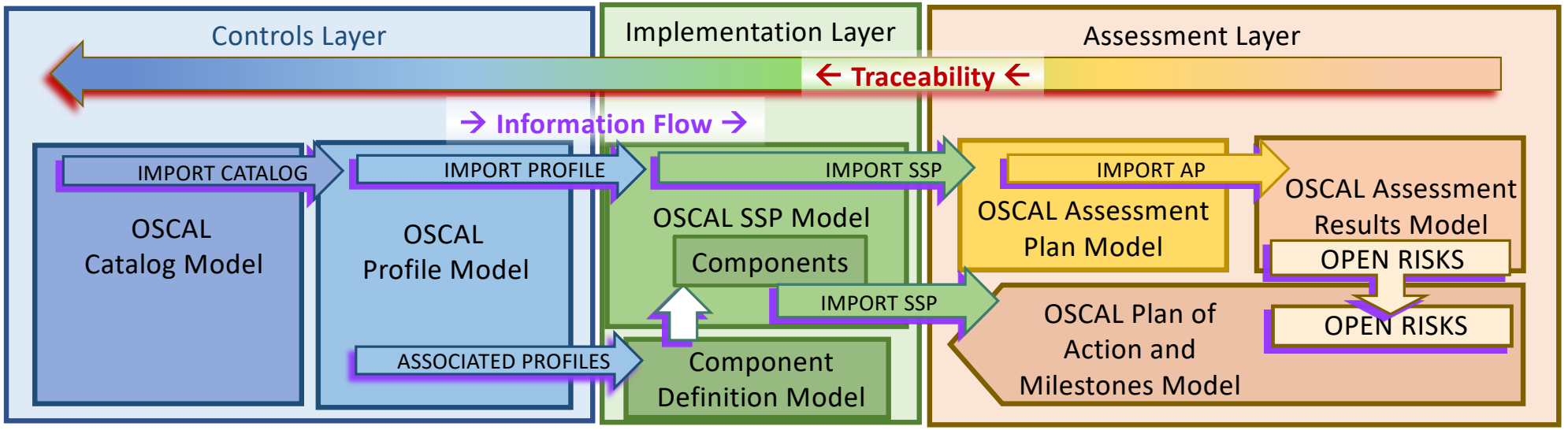
OSCAL 101 Series - Lecture #4

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

Presenter: **Dr. Michaela Iorga**
OSCAL Strategic Outreach Director

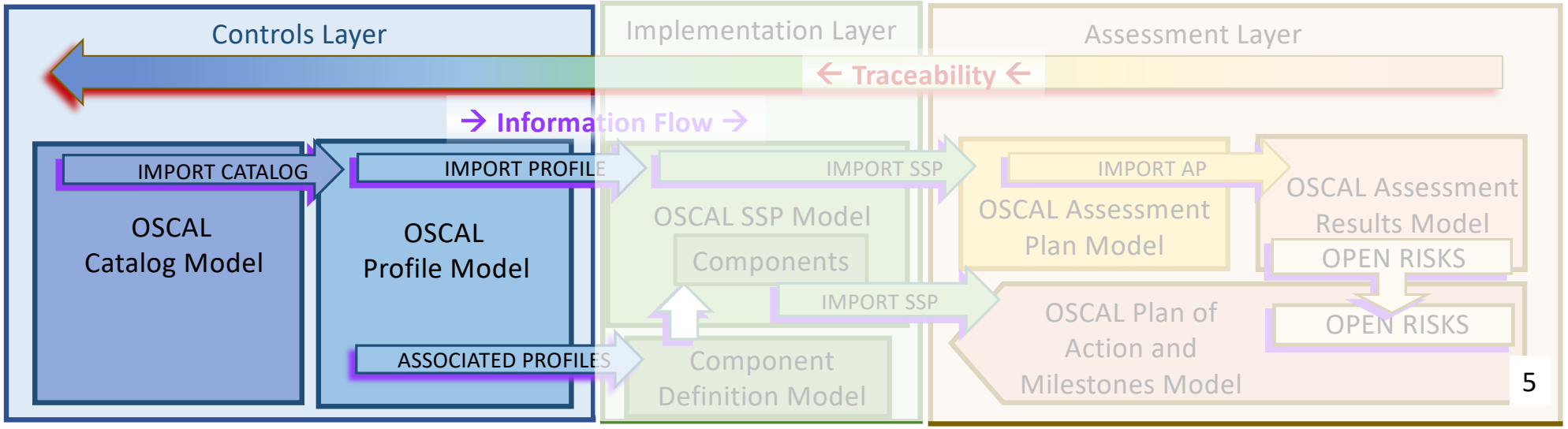
Recap: OSCAL Layers

- OSCAL is a standardized, flexible, open-source language designed to express security controls and their associated implementations and assessment methods in machine-readable formats (XML, JSON, and YAML). OSCAL content can be easily transformed into human-friendly formats.
- OSCAL:
  - Enables automated traceability
  - Provides a standards-based foundation for the next generation GRCs
  - Helps improve the risk management posture, consistency, and interoperability.



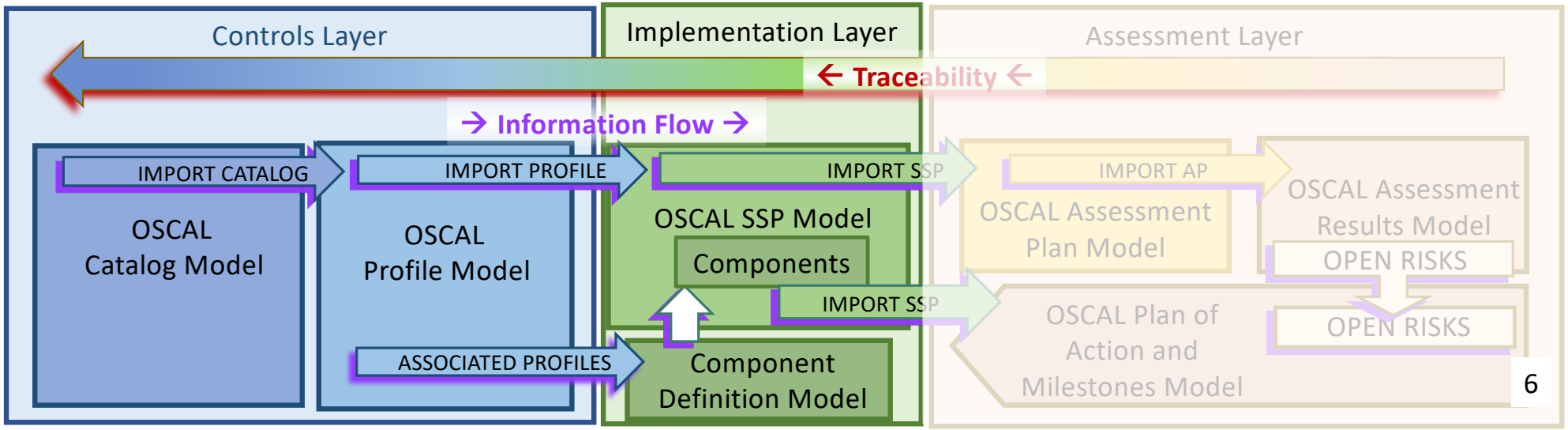
Recap: OSCAL Control Layer

- OSCAL is a standardized, flexible, open-source language designed to express security controls and their associated implementations and assessment methods in machine-readable formats (XML, JSON, and YAML). OSCAL content can be easily transformed into human-friendly formats.
- OSCAL:
  - Enables automated traceability
  - Provides a standards-based foundation for the next generation GRCs
  - Helps improve the risk management posture, consistency, and interoperability.



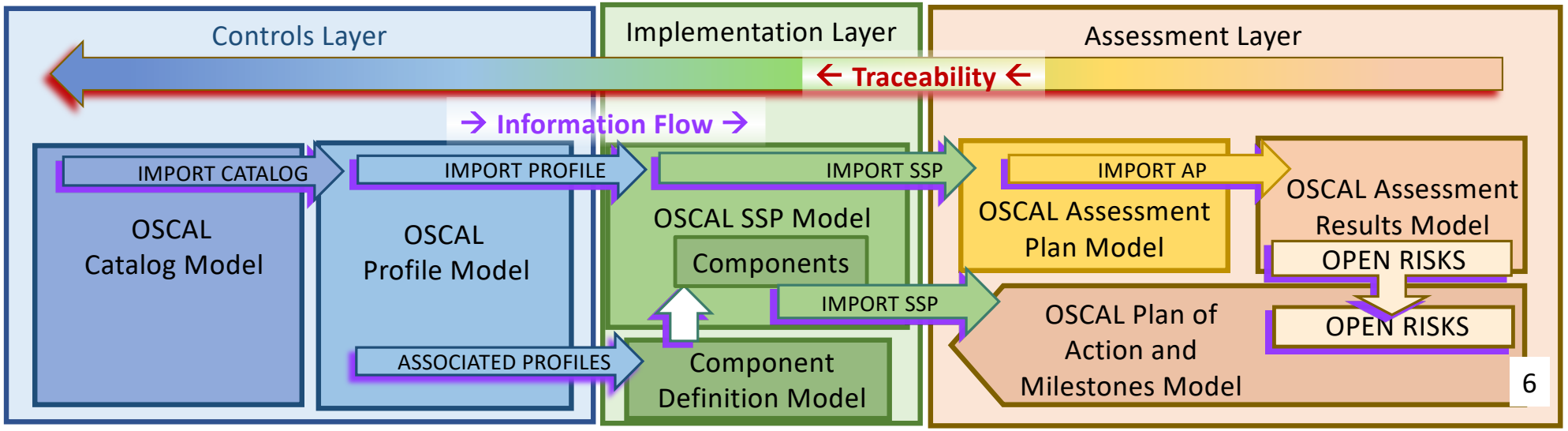
Recap: OSCAL Implementation Layer

- OSCAL is a standardized, flexible, open-source language designed to express security controls and their associated implementations and assessment methods in machine-readable formats (XML, JSON, and YAML). OSCAL content can be easily transformed into human-friendly formats.
- OSCAL:
  - Enables automated traceability
  - Provides a standards-based foundation for the next generation GRCs
  - Helps improve the risk management posture, consistency, and interoperability.

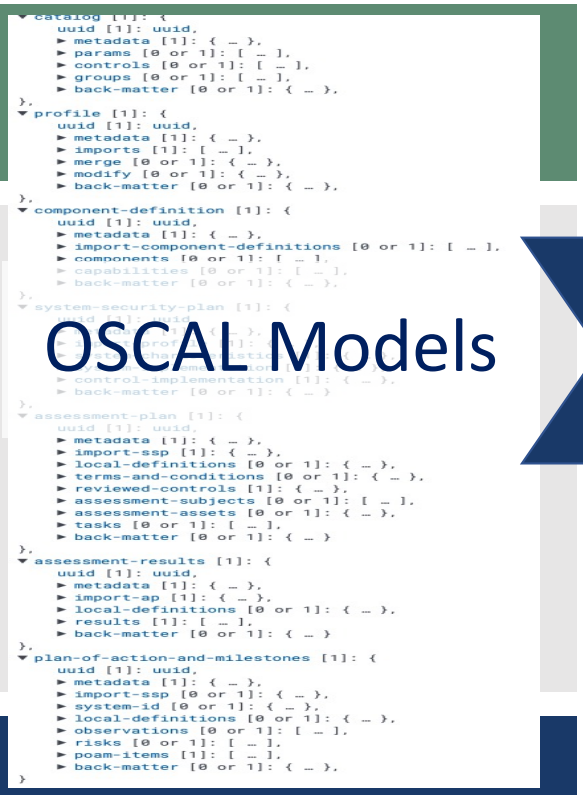


Today: OSCAL Assessment Layer

- OSCAL is a standardized, flexible, open-source language designed to express security controls and their associated implementations and assessment methods in machine-readable formats (XML, JSON, and YAML). OSCAL content can be easily transformed into human-friendly formats.
- OSCAL:
  - Enables automated traceability
  - Provides a standards-based foundation for the next generation GRCs
  - Helps improve the risk management posture, consistency, and interoperability.



Recap: OSCAL Models >>> OSCAL Content >>> OSCAL Tools



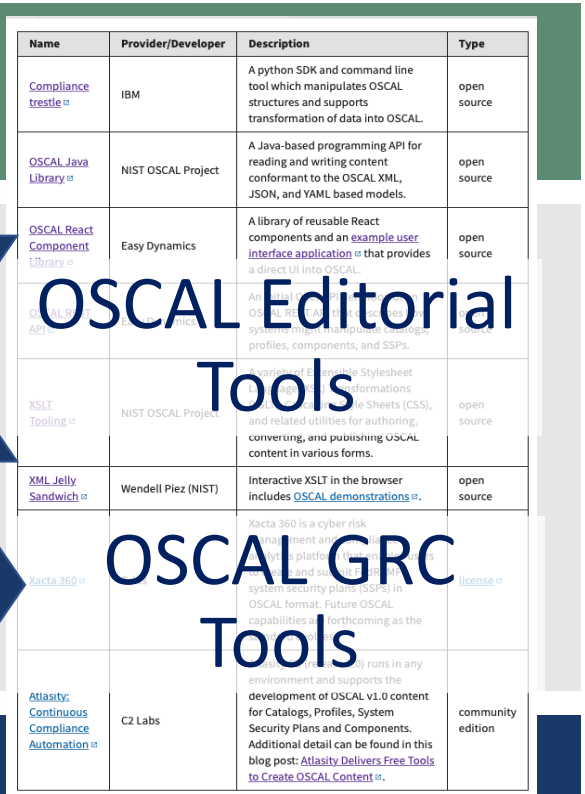
OSCAL Models

https://github.com/usnistgov/OSCAL

OSCAL Content Generation

OSCAL Content in Action

https://github.com/usnistgov/oscal-content



Name	Provider/Developer	Description	Type
Compliance trestle	IBM	A python SDK and command line tool which manipulates OSCAL structures and supports transformation of data into OSCAL.	open source
OSCAL Java Library	NIST OSCAL Project	A Java-based programming API for reading and writing content conformant to the OSCAL XML, JSON, and YAML based models.	open source
OSCAL React Component Library	Easy Dynamics	A library of reusable React components and an example user interface application that provides a direct UI into OSCAL	open source
XSLT Tooling	NIST OSCAL Project		open source
XML Jelly Sandwich	Wendell Piez (NIST)	Interactive XSLT in the browser includes OSCAL demonstrations.	open source
Xacta 360			license
Atlasity: Continuous Compliance Automation	C2 Labs	development of OSCAL v1.0 content for Catalogs, Profiles, System Security Plans and Components. Additional detail can be found in this blog post: Atlasity Delivers Free Tools to Create OSCAL Content.	community edition

OSCAL Editorial Tools

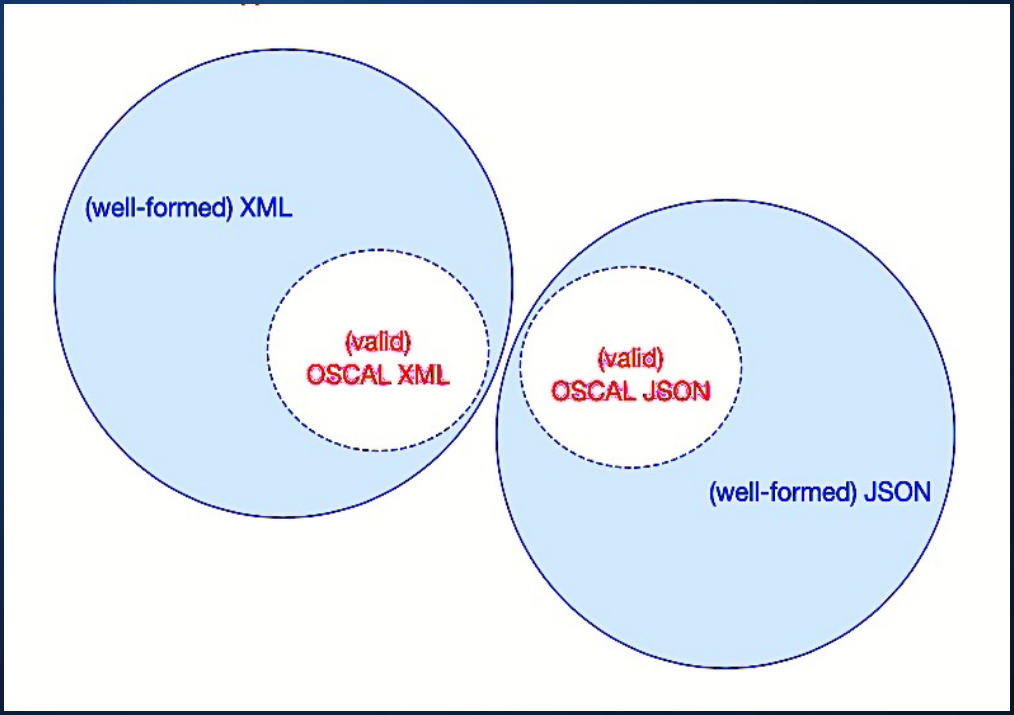
OSCAL GRC Tools

https://github.com/usnistgov/oscal-tools

Recap - OSCAL Content Validation

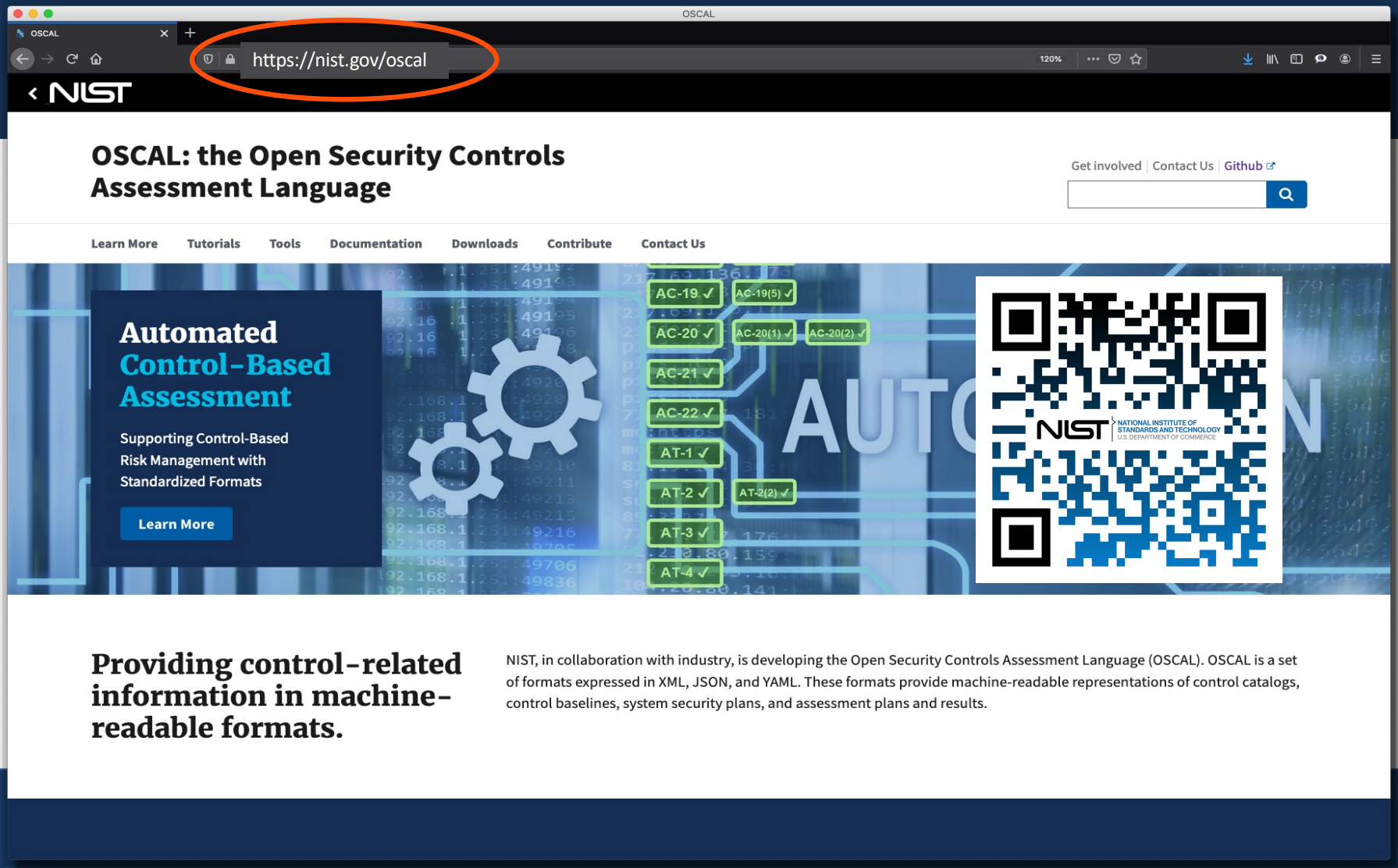
https://pages.nist.gov/OSCAL/concepts/validation/

"well-formed" vs "valid" OSCAL content



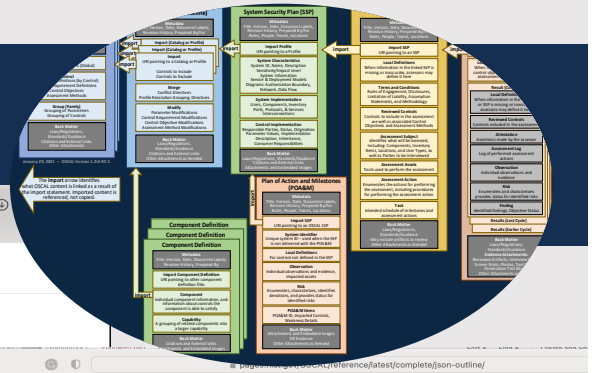
XML Schema Validators:
https://www.w3.org/XML/Schema#Tools

JSON Schema Validators:
https://json-schema.org/implementations.html#validators


OSCAL
https://nist.gov/oscal
NIST
OSCAL: the Open Security Controls Assessment Language
Get involved | Contact Us | Github
Learn More Tutorials Tools Documentation Downloads Contribute Contact Us
Automated Control-Based Assessment
Supporting Control-Based Risk Management with Standardized Formats
Learn More
AC-19 ✓
AC-19(5) ✓
AC-20 ✓
AC-20(1) ✓
AC-20(2) ✓
AC-21 ✓
AC-22 ✓
AT-1 ✓
AT-2 ✓
AT-2(2) ✓
AT-3 ✓
AT-4 ✓
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
Providing control-related information in machine-readable formats.
NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.

Recap: OSCAL Models' Outline

https://pages.nist.gov/OSCAL/reference/latest/complete/xml-outline/



OSCAL

About Learn Concepts Reference Downloads Tools Contribute Contact Us

- Model Reference
- Data Types
- Release Notes
- Development Snapshot
- Latest Release (v1.0.4)
- All Models
  - JSON Outline
  - JSON Reference
  - JSON Index
  - JSON Metaschema Reference
  - XML Outline
  - XML Reference
  - XML Index
  - XML Metaschema Reference
  - Assessment Plan Model
  - Assessment Results Model
  - Catalog Model
  - Component Definition Model
  - Plan of Action and Milestones Model

Complete v1.0.4 XML Format Outline

The following outline is a representation of the XML format for the combination of all OSCAL models. For each element or attribute, see the corresponding entry in the XML Format Reference. The cardinality and data type are also provided for each element or attribute.

```
▼ <catalog uuid="uuid"> [1]
    ▶ <metadata> … </metadata> [1]
    ▶ <param id="token" class="token" depends-on="token"> … </param> [0 to ∞]
    ▶ <control id="token" class="token"> … </control> [0 to ∞]
    ▶ <group id="token" class="token"> … </group> [0 to ∞]
    ▶ <back-matter> … </back-matter> [0 or 1]
</catalog>
▼ <profile uuid="uuid"> [1]
    ▶ <metadata> … </metadata> [1]
    ▶ <import href="uri-reference"> … </import> [1 to ∞]
    ▶ <merge> … </merge> [0 or 1]
    ▶ <modify> … </modify> [0 or 1]
    ▶ <back-matter> … </back-matter> [0 or 1]
</profile>
▼ <component-definition uuid="uuid"> [1]
    ▶ <metadata> … </metadata> [1]
    ▶ <import-component-definition href="uri-reference"/> [0 to ∞]
    ▶ <component uuid="uuid" type="string"> … </component> [0 to ∞]
    ▶ <capability uuid="uuid" name="string"> … </capability> [0 to ∞]
    ▶ <back-matter> … </back-matter> [0 or 1]
</component-definition>
▼ <system-security-plan uuid="uuid"> [1]
    ▶ <metadata> … </metadata> [1]
    ▶ <import-profile href="uri-reference"> … </import-profile> [1]
    ▶ <system-characteristics> … </system-characteristics> [1]
    ▶ <system-implementation> … </system-implementation> [1]
    ▶ <control-implementation> … </control-implementation> [1]
    ▶ <back-matter> … </back-matter> [0 or 1]
</system-security-plan>
▶ <assessment-plan uuid="uuid"> … </assessment-plan> [1]
▶ <assessment-results uuid="uuid"> … </assessment-results> [1]
▶ <plan-of-action-and-milestones uuid="uuid"> … </plan-of-action-and-milestones> [1]
```


…./complete/json-outline/

NIST

OSCAL

About Learn Concepts Reference Downloads Tools Contribute

- Model Reference
- Data Types
- Release Notes
- Development Snapshot
- Latest Release (v1.0.4)
- All Models
  - JSON Outline
  - JSON Reference
  - JSON Index
  - JSON Metaschema Reference
  - XML Outline
  - XML Reference
  - XML Index
  - XML Metaschema Reference
  - Assessment Plan Model
  - Assessment Results Model
  - Catalog Model
  - Component Definition Model

Complete v1.0.4 JSON Format Outline

The following outline is a representation of the JSON format for the combination of all OSCAL models. For each property, see the corresponding entry in the JSON Format Reference. The cardinality and data type are also provided for each property where appropriate.

```
▼ catalog [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ params [0 or 1]: [ … ],
    ▶ controls [0 or 1]: [ … ],
    ▶ groups [0 or 1]: [ … ],
    ▶ back-matter [0 or 1]: { … },
},
▼ profile [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ imports [1]: [ … ],
    ▶ merge [0 or 1]: { … },
    ▶ modify [0 or 1]: { … },
    ▶ back-matter [0 or 1]: { … },
},
▼ component-definition [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-component-definitions [0 or 1]: [ … ],
    ▶ components [0 or 1]: [ … ],
    ▶ capabilities [0 or 1]: [ … ],
    ▶ back-matter [0 or 1]: { … },
},
▼ system-security-plan [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-profile [1]: { … },
    ▶ system-characteristics [1]: { … },
    ▶ system-implementation [1]: { … },
    ▶ control-implementation [1]: { … },
```

Recap - Common OSCAL Structure

Complete v1.0.4 JSON Format Outline

The following outline is a representation of the JSON format for the combination of all OSCAL models. For each p
in the JSON Format Reference. The cardinality and data type are also provided for each property where appropriat

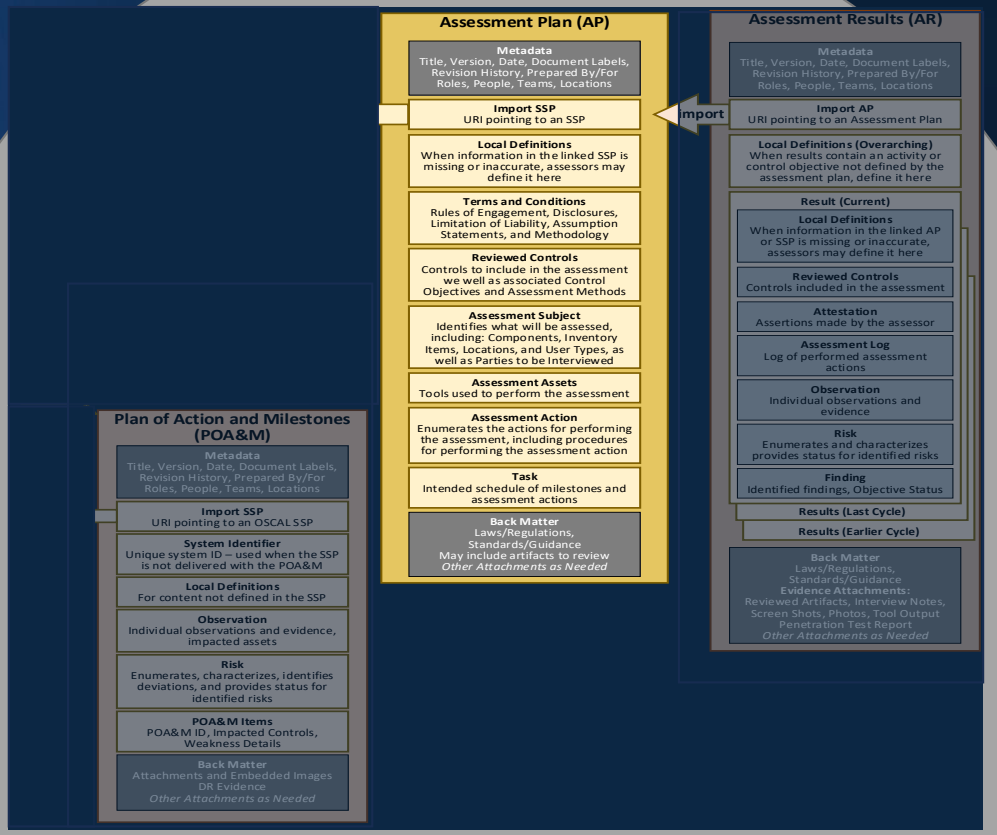
```
▼ catalog [1]: {                                   Root Element & Root UUID
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ params [0 or 1]: [ … ],
    ▶ controls [0 or 1]: [ … ],                    Body (Model Specific)
    ▶ groups [0 or 1]: [ … ],
    ▶ back-matter [0 or 1]: { … },
},
▼ profile [1]: {                                   Root Element & Root UUID
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ imports [1]: [ … ],
    ▶ merge [0 or 1]: { … },                       Body (Model Specific)
    ▶ modify [0 or 1]: { … },
    ▶ back-matter [0 or 1]: { … },
},
▼ component-definition [1]: {                      Root Element & Root UUID
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-component-definitions [0 or 1]: [ … ],
    ▶ components [0 or 1]: [ … ],                  Body (Model Specific)
    ▶ capabilities [0 or 1]: [ … ],
    ▶ back-matter [0 or 1]: { … },
}
```

OSCAL Assessment Layer

Assessment Plan Model

Assessment Results Model

Plan of Actions & Milestones



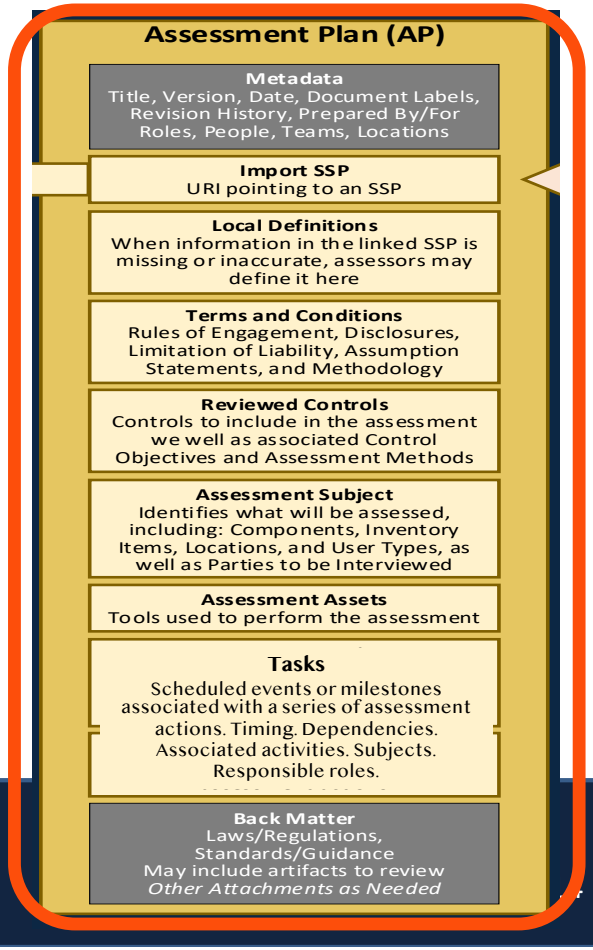
The Anatomy of the Assessment Plan (AP) Model

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

Assessment Plan Model v1.0.4 JSON Format Outline

The following outline is a representation of the JSON format for this model. For each property, the name links to the corresponding entry in the JSON Format Reference. The cardinality and data type are also provided for each property where appropriate.

```
▼ assessment-plan [1]: {
    uuid [1]: uuid,
  ▶ metadata [1]: { … },
  ▶ import-ssp [1]: { … },
  ▶ local-definitions [0 or 1]: { … },
  ▶ terms-and-conditions [0 or 1]: { … },
  ▶ reviewed-controls [1]: { … },
  ▶ assessment-subjects [0 or 1]: [ … ],
  ▶ assessment-assets [0 or 1]: { … },
  ▶ tasks [0 or 1]: [ … ],
  ▶ back-matter [0 or 1]: { … }
}
```



The Anatomy of the Assessment Plan - Body

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-reference/#/assessment-plan

assessment-plan

object (global definition)

Switch to XML

Security Assessment Plan (SAP)

DESCRIPTION An assessment plan, such as those provided by a FedRAMP assessor.

▼ Properties (10)

uuid

uuid [1]

Switch to XML

Assessment Plan Universally Unique Identifier

DESCRIPTION A machine-oriented, globally unique identifier with cross-instance scope that can be used to reference this assessment plan in this or other OSCAL instances. The locally defined *UUID* of the `assessment plan` can be used to reference the data item locally or globally (e.g., in an imported OSCAL instance). This UUID should be assigned per-subject, which means it should be consistently used to identify the same subject across revisions of the document.

metadata

object (global definition) [1]

Switch to XML

Publication metadata

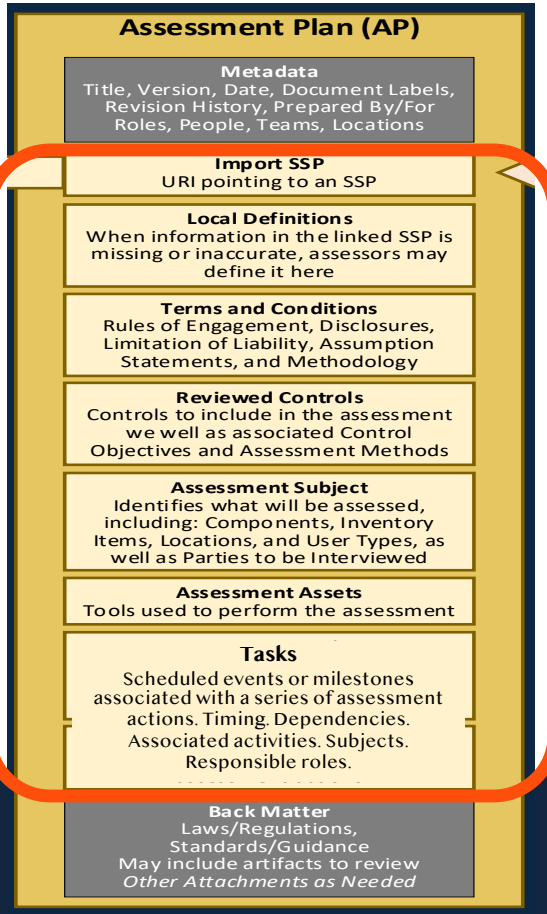
DESCRIPTION Provides information about the publication and availability of the containing document.

The Anatomy of the Assessment Plan- Body

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

```
▼ assessment-plan [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-ssp [1]: { … },
    ▶ local-definitions [0 or 1]: { … },
    ▶ terms-and-conditions [0 or 1]: { … },
    ▶ reviewed-controls [1]: { … },
    ▶ assessment-subjects [0 or 1]: [ … ],
    ▶ assessment-assets [0 or 1]: { … },
    ▶ tasks [0 or 1]: [ … ],
    ▶ back-matter [0 or 1]: { … }
}
```

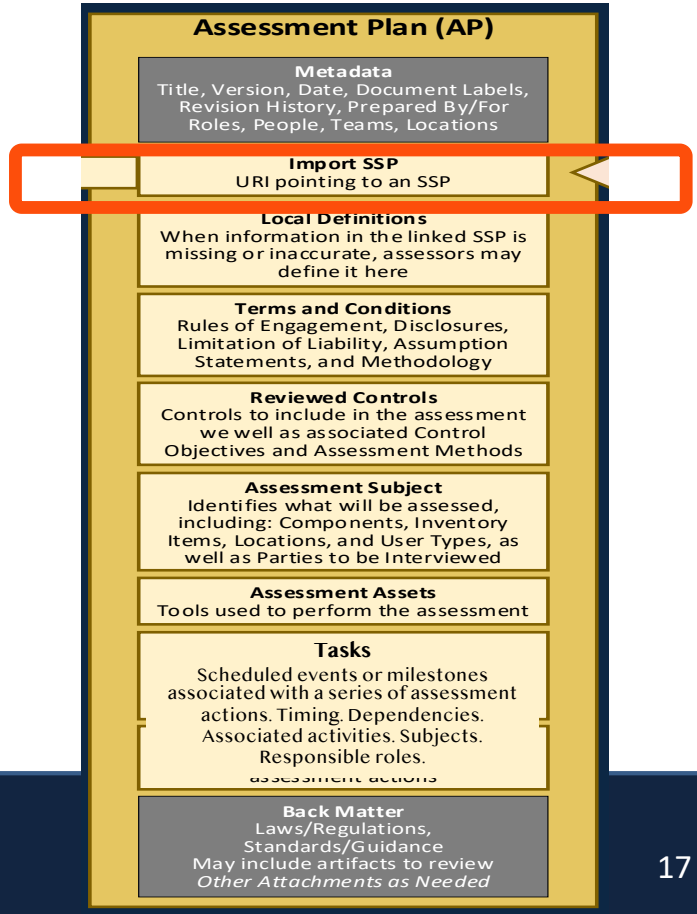
Root Element & Root UUID



The Anatomy of the Assessment Plan - Import

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

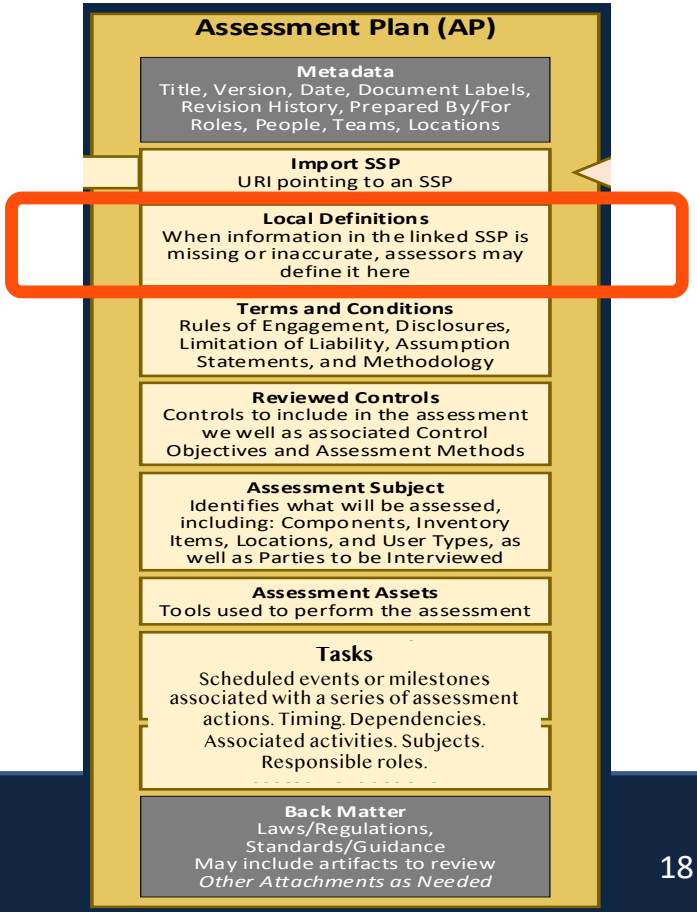
```
▼ assessment-plan [1]: {
    uuid [1]: uuid,
  ▶ metadata [1]: { … },
  ▼ import-ssp [1]: {
      href [1]: uri-reference,
      remarks [0 or 1]: markup-multiline,
    },
  ▶ local-definitions [0 or 1]: { … },
  ▶ terms-and-conditions [0 or 1]: { … },
  ▶ reviewed-controls [1]: { … },
  ▶ assessment-subjects [0 or 1]: [ … ],
  ▶ assessment-assets [0 or 1]: { … },
  ▶ tasks [0 or 1]: [ … ],
  ▶ back-matter [0 or 1]: { … }
}
```



The Anatomy of the Assessment Plan – Local Definitions

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

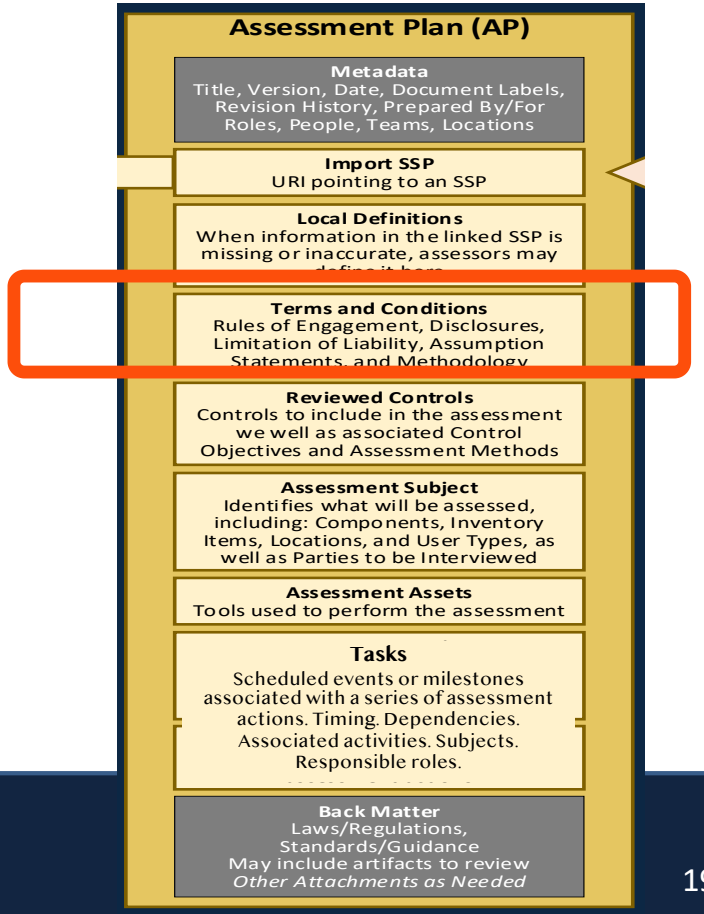
```
▼ assessment-plan [1]: {
    uuid [1]: uuid,
  ▶ metadata [1]: { … },
  ▶ import-ssp [1]: { … },
  ▼ local-definitions [0 or 1]: {
      ▶ components [0 or 1]: [ … ],
      ▶ inventory-items [0 or 1]: [ … ],
      ▶ users [0 or 1]: [ … ],
      ▶ objectives-and-methods [0 or 1]: [ … ],
      ▶ activities [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline,
    },
  ▶ terms-and-conditions [0 or 1]: { … },
  ▶ reviewed-controls [1]: { … },
  ▶ assessment-subjects [0 or 1]: [ … ],
  ▶ assessment-assets [0 or 1]: { … },
  ▶ tasks [0 or 1]: [ … ],
  ▶ back-matter [0 or 1]: { … }
}
```



The Anatomy of the Assessment Plan – Terms & Conditions

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

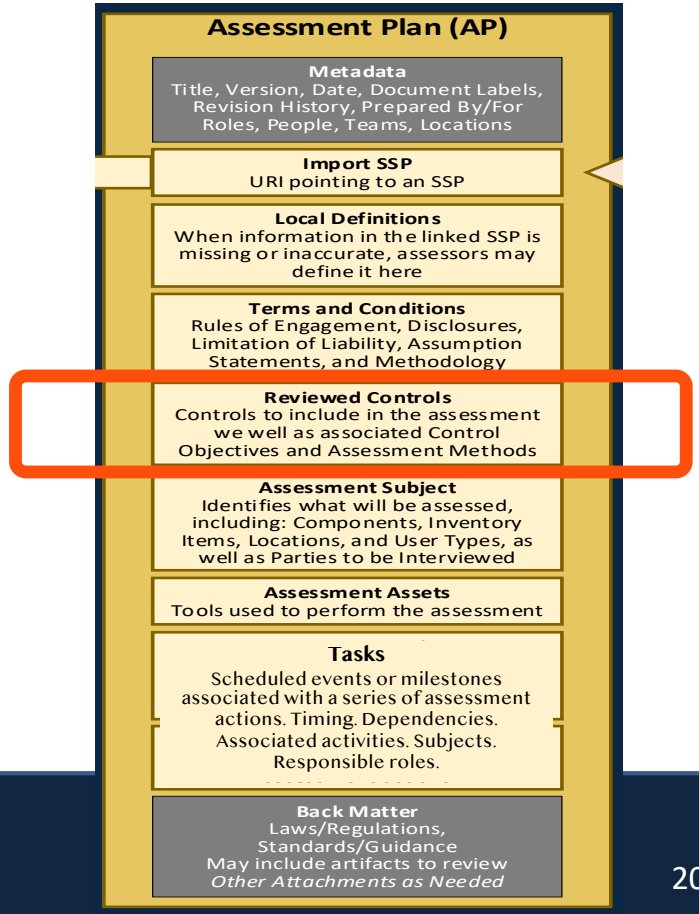
```
▼ assessment-plan [1]: {
    uuid [1]: uuid,
  ▶ metadata [1]: { … },
  ▶ import-ssp [1]: { … },
  ▶ local-definitions [0 or 1]: { … },
  ▼ terms-and-conditions [0 or 1]: {
      ▼ parts [0 or 1]: [
          An array of part objects [1 to ∞] {
              uuid [0 or 1]: uuid,
              name [1]: token,
              ns [0 or 1]: uri,
              class [0 or 1]: token,
              title [0 or 1]: markup-line,
            ▶ props [0 or 1]: [ … ],
              prose [0 or 1]: markup-multiline,
            ▶ parts [0 or 1]: [ … ],
            ▶ links [0 or 1]: [ … ],
          }
      ],
  },
  ▶ reviewed-controls [1]: { … },
  ▶ assessment-subjects [0 or 1]: [ … ],
```



The Anatomy of the Assessment Plan – Reviewed Controls

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

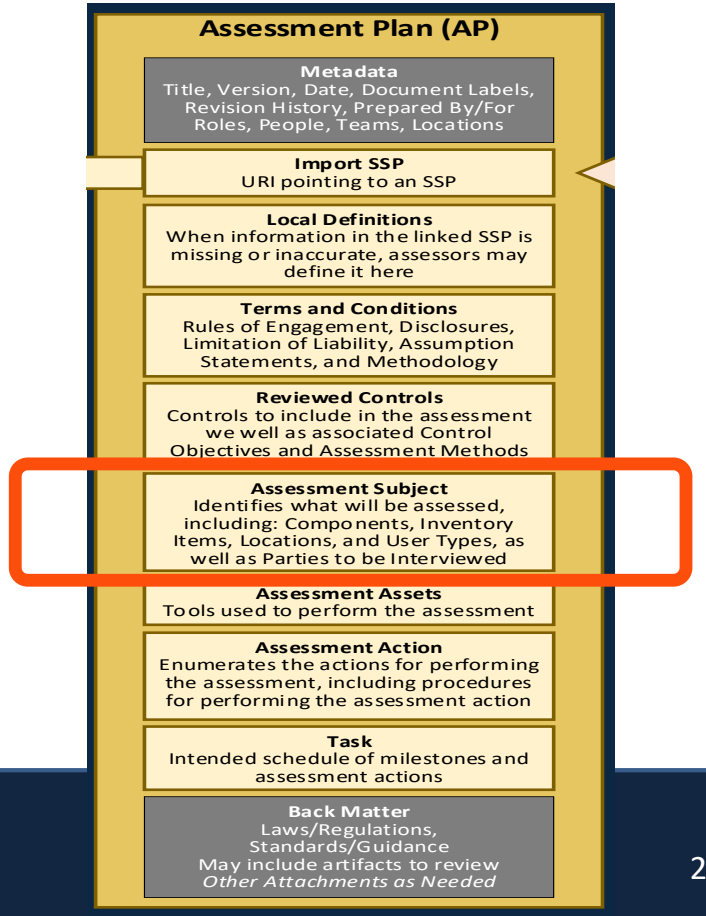
```
▼ reviewed-controls [1]: {
    description [0 or 1]: markup-multiline,
    ▶ props [0 or 1]: [ … ],
    ▶ links [0 or 1]: [ … ],
    ▼ control-selections [1]: [
        An array of control-selection objects [1 to ∞] {
            description [0 or 1]: markup-multiline,
            ▶ props [0 or 1]: [ … ],
            ▶ links [0 or 1]: [ … ],
            A choice of:
              ▶ include-all [1]: { … },
              ▶ include-controls [1]: [ … ]
            ▶ exclude-controls [0 or 1]: [ … ],
            remarks [0 or 1]: markup-multiline,
        }
    ],
    ▼ control-objective-selections [0 or 1]: [
        An array of control-objective-selection objects [1 to ∞] {
            description [0 or 1]: markup-multiline,
            ▶ props [0 or 1]: [ … ],
            ▶ links [0 or 1]: [ … ],
            A choice of:
              ▶ include-all [1]: { … },
              ▶ include-objectives [1]: [ … ]
            ▶ exclude-objectives [0 or 1]: [ … ],
            remarks [0 or 1]: markup-multiline,
        }
    ],
    remarks [0 or 1]: markup-multiline,
}
```



The Anatomy of the Assessment Plan – Assessment Subject

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

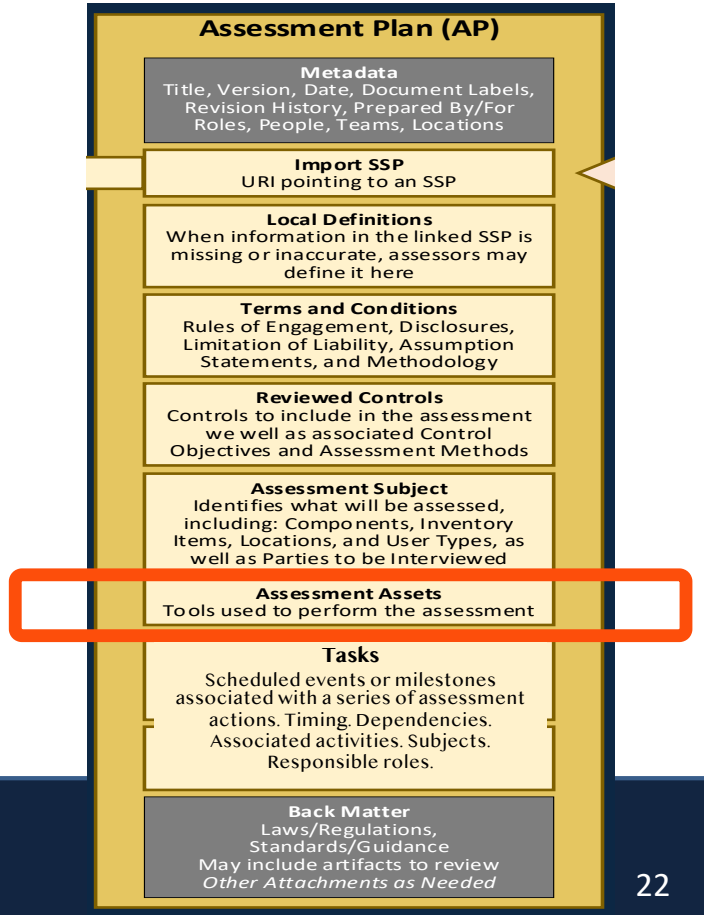
```
▼ assessment-subjects [0 or 1]: [
    An array of assessment-subject objects [1 to ∞] {
        type [1]: token,
        description [0 or 1]: markup-multiline,
        ▶ props [0 or 1]: [ … ],
        ▶ links [0 or 1]: [ … ],
        A choice of:
          ▶ include-all [1]: { … },
          ▼ include-subjects [1]: [
              An array of include-subject objects [1 to ∞] {
                  subject-uuid [1]: uuid,
                  type [1]: token,
                  ▶ props [0 or 1]: [ … ],
                  ▶ links [0 or 1]: [ … ],
                  remarks [0 or 1]: markup-multiline
              }
          ]
        ▼ exclude-subjects [0 or 1]: [
            An array of exclude-subject objects [1 to ∞] {
                subject-uuid [1]: uuid,
                type [1]: token,
                ▶ props [0 or 1]: [ … ],
                ▶ links [0 or 1]: [ … ],
                remarks [0 or 1]: markup-multiline
            }
        ],
        remarks [0 or 1]: markup-multiline,
    }
],
▶ assessment-assets [0 or 1]: { … },
```



The Anatomy of the Assessment Plan – Assessment Assets

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

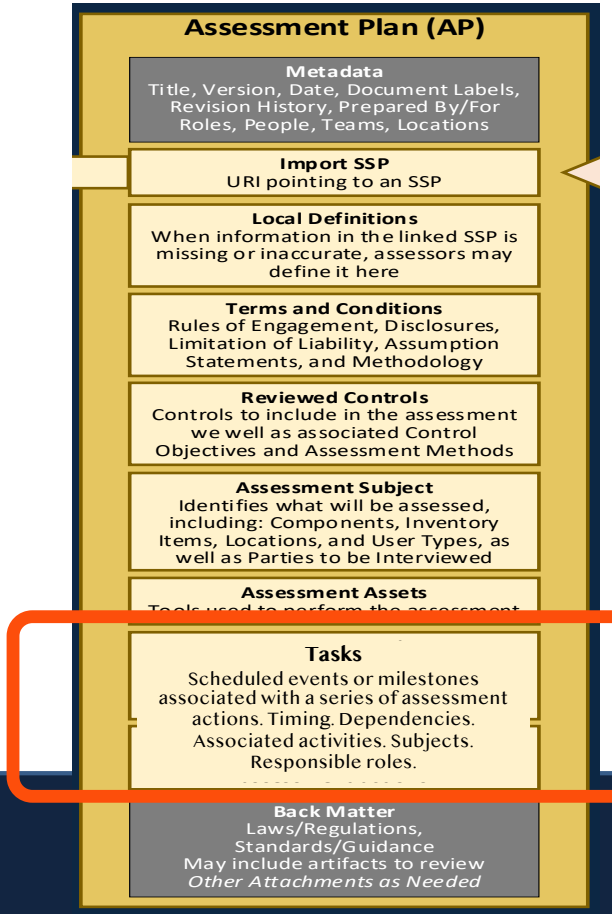
```
▶ reviewed-controls [1]: { … },
▶ assessment-subjects [0 or 1]: [ … ],
▼ assessment-assets [0 or 1]: {
    ▼ components [0 or 1]: [
        An array of component objects [1 to ∞] {
            uuid [1]: uuid,
            type [1]: string,
            title [1]: markup-line,
            description [1]: markup-multiline,
            purpose [0 or 1]: markup-line,
            ▶ props [0 or 1]: [ … ],
            ▶ links [0 or 1]: [ … ],
            ▶ status [1]: { … },
            ▶ responsible-roles [0 or 1]: [ … ],
            ▶ protocols [0 or 1]: [ … ],
            remarks [0 or 1]: markup-multiline,
        }
    ],
    ▼ assessment-platforms [1]: [
        An array of assessment-platform objects [1 to ∞] {
            uuid [1]: uuid,
            title [0 or 1]: markup-line,
            ▶ props [0 or 1]: [ … ],
            ▶ links [0 or 1]: [ … ],
            ▶ uses-components [0 or 1]: [ … ],
            remarks [0 or 1]: markup-multiline
        }
    ],
}
▶ tasks [0 or 1]: [ … ],
```



The Anatomy of the Assessment Plan – Task

https://pages.nist.gov/OSCAL/reference/latest/assessment-plan/json-outline/

```
▼ tasks [0 or 1]: [
    An array of task objects [1 to ∞] {
        uuid [1]: uuid,
        type [1]: token,
        title [1]: markup-line,
        description [0 or 1]: markup-multiline,
      ▶ props [0 or 1]: [ … ],
      ▶ links [0 or 1]: [ … ],
      ▶ timing [0 or 1]: { … },
      ▶ dependencies [0 or 1]: [ … ],
      ▶ tasks [0 or 1]: [ … ],
      ▼ associated-activities [0 or 1]: [
            An array of associated-activity objects [1 to ∞] {
                activity-uuid [1]: uuid,
              ▶ props [0 or 1]: [ … ],
              ▶ links [0 or 1]: [ … ],
              ▶ responsible-roles [0 or 1]: [ … ],
              ▶ subjects [1]: [ … ],
                remarks [0 or 1]: markup-multiline,
            }
        ],
      ▼ subjects [0 or 1]: [
            An array of subject objects [1 to ∞] {
                type [1]: token,
                description [0 or 1]: markup-multiline,
              ▶ props [0 or 1]: [ … ],
              ▶ links [0 or 1]: [ … ],
                A choice of:
                  ▶ include-all [1]: { … },
                  ▶ include-subjects [1]: [ … ]
              ▶ exclude-subjects [0 or 1]: [ … ],
                remarks [0 or 1]: markup-multiline,
            }
        ],
      ▶ responsible-roles [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline
    }
```

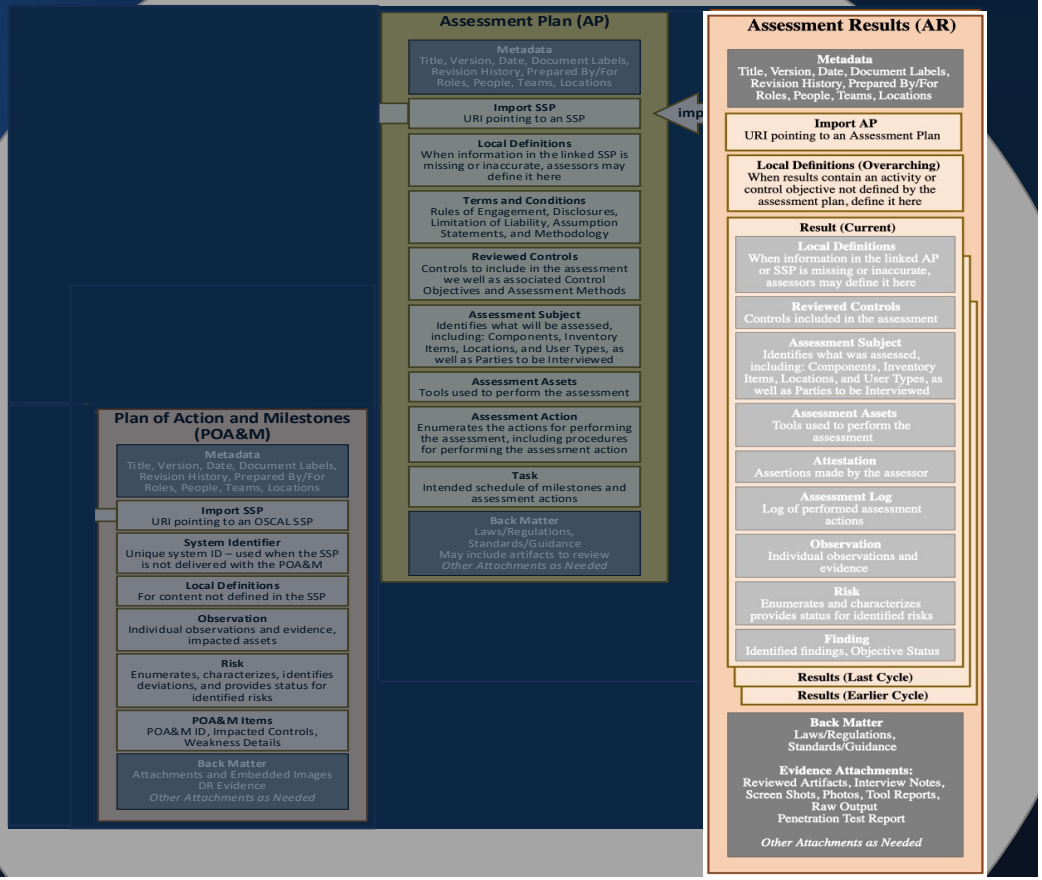


OSCAL Assessment Layer

Assessment Plan Model

Assessment Results Model

Plan of Actions & Milestones



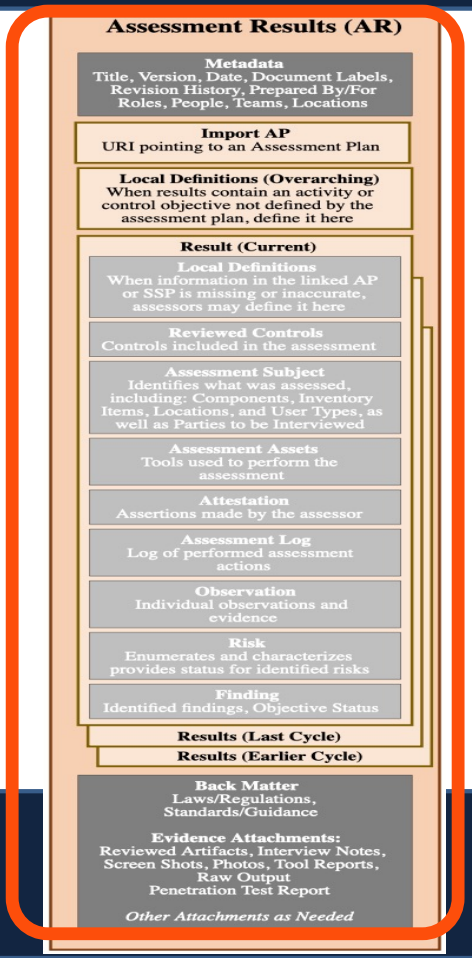
The Anatomy of the Assessment Results Model – Body

https://pages.nist.gov/OSCAL/reference/latest/assessment-results/json-outline/

Assessment Results Model v1.0.4 JSON Format Outline

The following outline is a representation of the JSON format for this model. For each property, the name links to the corresponding entry in the JSON Format Reference. The cardinality and data type are also provided for each property where appropriate.

```
▼ assessment-results [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-ap [1]: { … },
    ▶ local-definitions [0 or 1]: { … },
    ▶ results [1]: [ … ],
    ▶ back-matter [0 or 1]: { … }
}
```

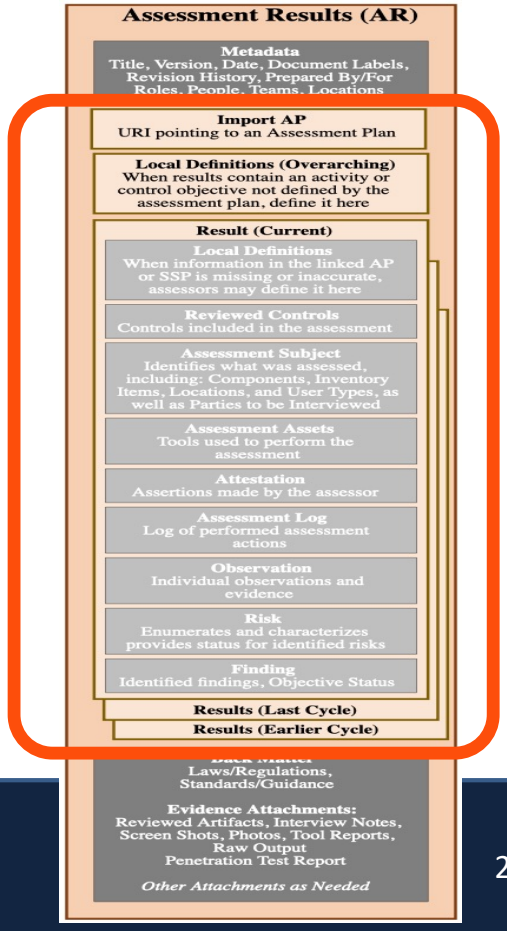


The Anatomy of the Assessment Results Model – Body

https://pages.nist.gov/OSCAL/reference/latest/assessment-results/json-outline/

```
▼ assessment-results [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-ap [1]: { … },
    ▶ local-definitions [0 or 1]: { … },
    ▶ results [1]: [ … ],
    ▶ back-matter [0 or 1]: { … }
}
```

Root Element & Root UUID

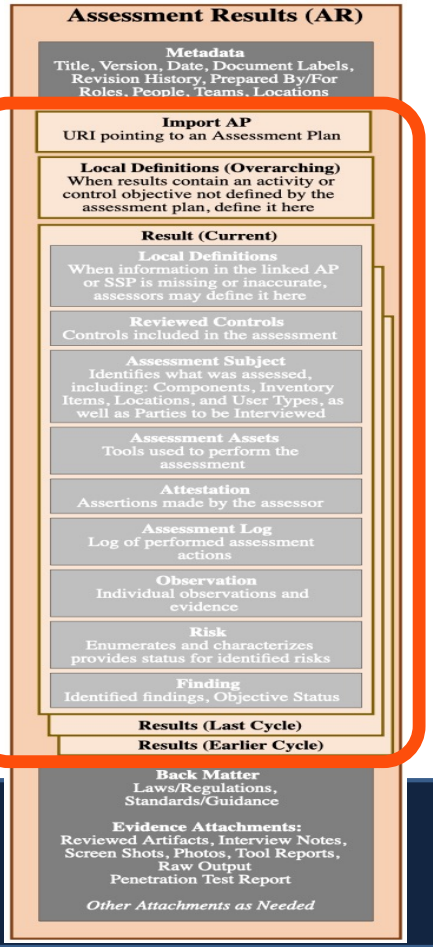


The Anatomy of the Assessment Results Model – Body

https://pages.nist.gov/OSCAL/reference/latest/assessment-results/json-outline/

```
▼ assessment-plan [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-ssp [1]: { … },
    ▼ local-definitions [0 or 1]: {
        ▶ components [0 or 1]: [ … ],
        ▶ inventory-items [0 or 1]: [ … ],
        ▶ users [0 or 1]: [ … ],
        ▶ objectives-and-methods [0 or 1]: [ … ],
        ▶ activities [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline,
    }
    ▶ terms-and-conditions [0 or 1]: { … },
    ▶ reviewed-controls [1]: { … },
    ▶ assessment-subjects [0 or 1]: [ … ],
    ▶ assessment-assets [0 or 1]: { … },
    ▶ tasks [0 or 1]: [ … ],
    ▶ back-matter [0 or 1]: { … }
}
```

```
▼ assessment-results [1]: {
    uuid [1]: uuid,
    ▶ import-ap [1]: { … },
    ▼ local-definitions [0 or 1]: {
        ▶ objectives-and-methods [0 or 1]: [ … ],
        ▶ activities [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline
    },
    ▼ results [1]: [
        An array of result objects [1 to ∞] {
            uuid [1]: uuid,
            title [1]: markup-line,
            description [1]: markup-multiline,
            start [1]: dateTime-with-timezone,
            end [0 or 1]: dateTime-with-timezone,
            ▶ props [0 or 1]: [ … ],
            ▶ links [0 or 1]: [ … ],
            ▼ local-definitions [0 or 1]: {
                ▶ components [0 or 1]: [ … ],
                ▶ inventory-items [0 or 1]: [ … ],
                ▶ users [0 or 1]: [ … ],
                ▶ assessment-assets [0 or 1]: { … },
                ▶ tasks [0 or 1]: [ … ],
            },
            ▶ reviewed-controls [1]: { … },
            ▶ attestations [0 or 1]: [ … ],
            ▶ assessment-log [0 or 1]: { … },
            ▶ observations [0 or 1]: [ … ],
            ▶ risks [0 or 1]: [ … ],
            ▶ findings [0 or 1]: [ … ],
            remarks [0 or 1]: markup-multiline
        }
    ]
    ▶ back-matter [0 or 1]: { … }
}
```

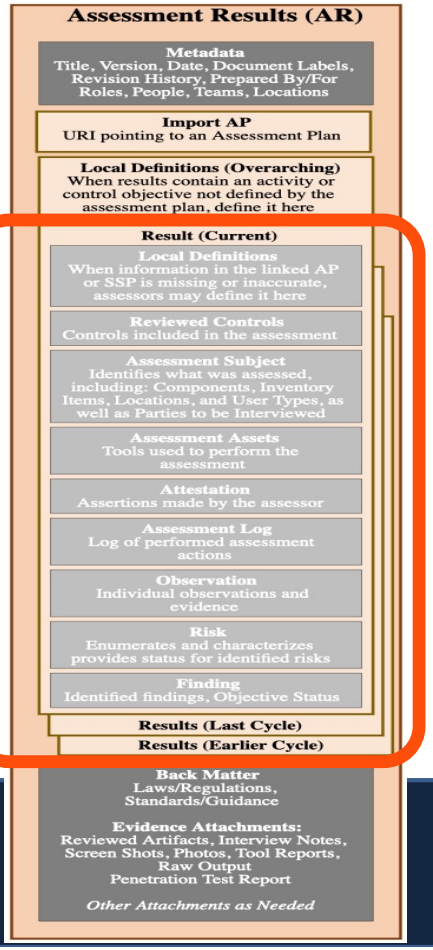


The Anatomy of the Assessment Results Model – Results

https://pages.nist.gov/OSCAL/reference/latest/assessment-results/json-outline/

```
▼ assessment-plan [1]: {
    uuid [1]: uuid,
  ▶ metadata [1]: { … },
  ▶ import-ssp [1]: { … },
  ▼ local-definitions [0 or 1]: {
      ▶ components [0 or 1]: [ … ],
      ▶ inventory-items [0 or 1]: [ … ],
      ▶ users [0 or 1]: [ … ],
      ▶ objectives-and-methods [0 or 1]: [ … ],
      ▶ activities [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline,
    },
  ▶ terms-and-conditions [0 or 1]: { … }
  ▶ reviewed-controls [1]: { … },
  ▶ assessment-subjects [0 or 1]: [ … ],
  ▶ assessment-assets [0 or 1]: { … },
  ▶ tasks [0 or 1]: [ … ],
  ▶ back-matter [0 or 1]: { … }
}
```

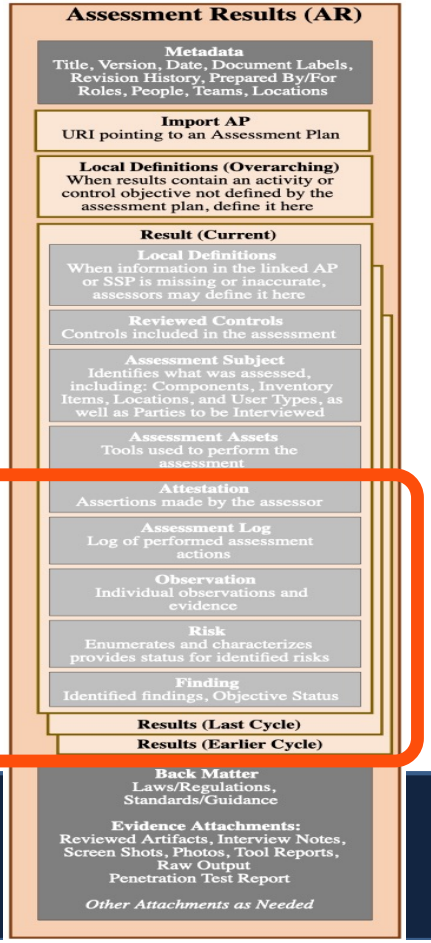
```
▼ results [1]: [
    An array of result objects [1 to ∞] {
        uuid [1]: uuid,
        title [1]: markup-line,
        description [1]: markup-multiline,
        start [1]: dateTime-with-timezone,
        end [0 or 1]: dateTime-with-timezone,
      ▶ props [0 or 1]: [ … ],
      ▶ links [0 or 1]: [ … ],
      ▼ local-definitions [0 or 1]: {
          ▶ components [0 or 1]: [ … ],
          ▶ inventory-items [0 or 1]: [ … ],
          ▶ users [0 or 1]: [ … ],
          ▶ assessment-assets [0 or 1]: { … },
          ▶ tasks [0 or 1]: [ … ],
        },
      ▶ reviewed-controls [1]: { … },
      ▶ attestations [0 or 1]: [ … ],
      ▶ assessment-log [0 or 1]: { … },
      ▶ observations [0 or 1]: [ … ],
      ▶ risks [0 or 1]: [ … ],
      ▶ findings [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline
    }
]
▶ back-matter [0 or 1]: { … }
}
```



The Anatomy of the Assessment Results Model – Results

https://pages.nist.gov/OSCAL/reference/latest/assessment-results/json-outline/

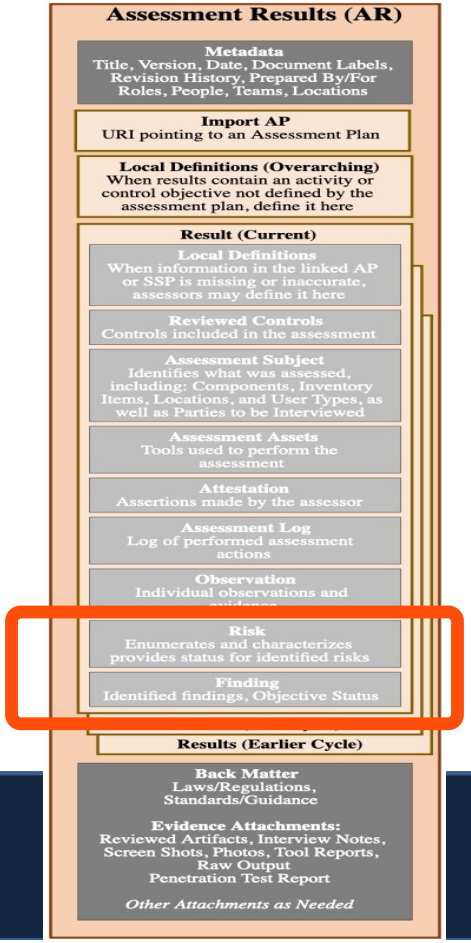
```
▶ local-definitions [0 or 1]: { … },
▼ attestations [0 or 1]: [
    An array of attestation objects [1 to ∞] {
        ▶ responsible-parties [0 or 1]: [ … ],
        ▶ parts [1]: [ … ],
    }
],
▶ assessment-log [0 or 1]: { … },
▼ observations [0 or 1]: [
    An array of observation objects [1 to ∞] {
        uuid [1]: uuid,
        title [0 or 1]: markup-line,
        description [1]: markup-multiline,
        ▶ props [0 or 1]: [ … ],
        ▶ links [0 or 1]: [ … ],
        ▶ methods [1]: [ … ],
        ▶ types [0 or 1]: [ … ],
        ▶ origins [0 or 1]: [ … ],
        ▶ subjects [0 or 1]: [ … ],
        ▶ relevant-evidence [0 or 1]: [ … ],
        collected [1]: dateTime-with-timezone,
        expires [0 or 1]: dateTime-with-timezone,
        remarks [0 or 1]: markup-multiline
    }
],
▶ risks [0 or 1]: [ … ],
▶ findings [0 or 1]: [ … ],
remarks [0 or 1]: markup-multiline
```



The Anatomy of the Assessment Results Model – Results

https://pages.nist.gov/OSCAL/reference/latest/assessment-results/json-outline/

```
▼ risks [0 or 1]: [
    An array of risk objects [1 to ∞] {
        uuid [1]: uuid,
        title [1]: markup-line,
        description [1]: markup-multiline,
        statement [1]: markup-multiline,
        ▶ props [0 or 1]: [ … ],
        ▶ links [0 or 1]: [ … ],
        status [1]: token,
        ▶ origins [0 or 1]: [ … ],
        ▶ threat-ids [0 or 1]: [ … ],
        ▶ characterizations [0 or 1]: [ … ],
        ▶ mitigating-factors [0 or 1]: [ … ],
        deadline [0 or 1]: dateTime-with-timezone,
        ▶ remediations [0 or 1]: [ … ],
        ▶ risk-log [0 or 1]: { … },
        ▶ related-observations [0 or 1]: [ … ],
    }
],
▼ findings [0 or 1]: [
    An array of finding objects [1 to ∞] {
        uuid [1]: uuid,
        title [1]: markup-line,
        description [1]: markup-multiline,
        ▶ props [0 or 1]: [ … ],
        ▶ links [0 or 1]: [ … ],
        ▶ origins [0 or 1]: [ … ],
        ▶ target [1]: { … },
        implementation-statement-uuid [0 or 1]: uuid,
        ▶ related-observations [0 or 1]: [ … ],
        ▶ related-risks [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline
    }
],
```

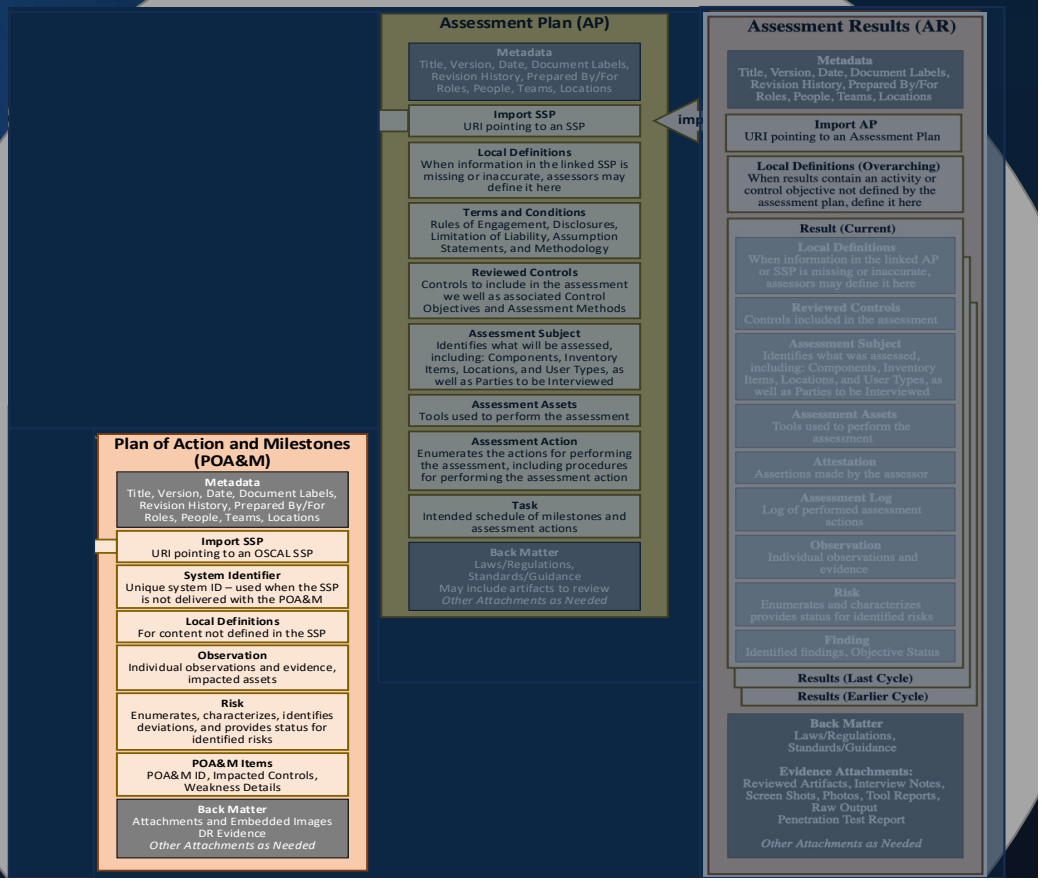


OSCAL Assessment Layer

Assessment Plan Model

Assessment Results Model

Plan of Actions & Milestones



The Anatomy of the POA&M Model – the Body

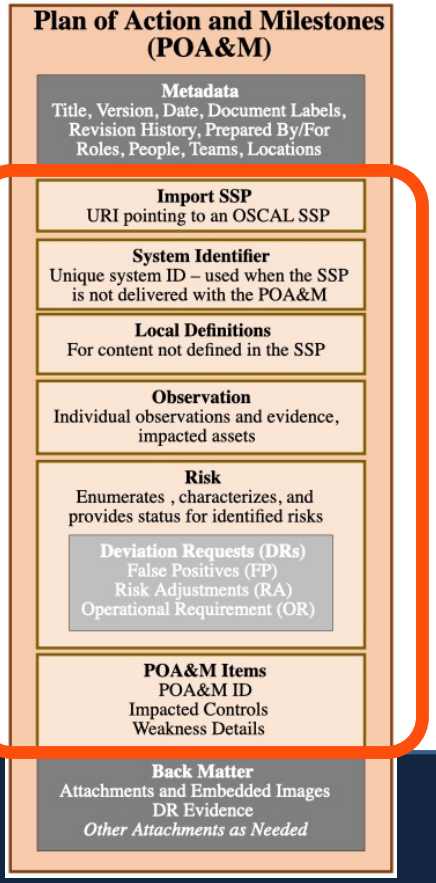
https://pages.nist.gov/OSCAL/reference/latest/plan-of-action-and-milestones/json-outline/

Plan of Action and Milestones Model v1.0.4 JSON Format Outline

The following outline is a representation of the JSON format for this model. For each property, the name links to the corresponding entry in the JSON Format Reference. The cardinality and data type are also provided for each property where appropriate.

```
▼ plan-of-action-and-milestones [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-ssp [0 or 1]: { … },
    ▶ system-id [0 or 1]: { … },
    ▶ local-definitions [0 or 1]: { … },
    ▶ observations [0 or 1]: [ … ],
    ▶ risks [0 or 1]: [ … ],
    ▶ poam-items [1]: [ … ],
    ▶ back-matter [0 or 1]: { … },
}
```

Root Element & Root UUID



The Anatomy of the POA&M Model – the Body

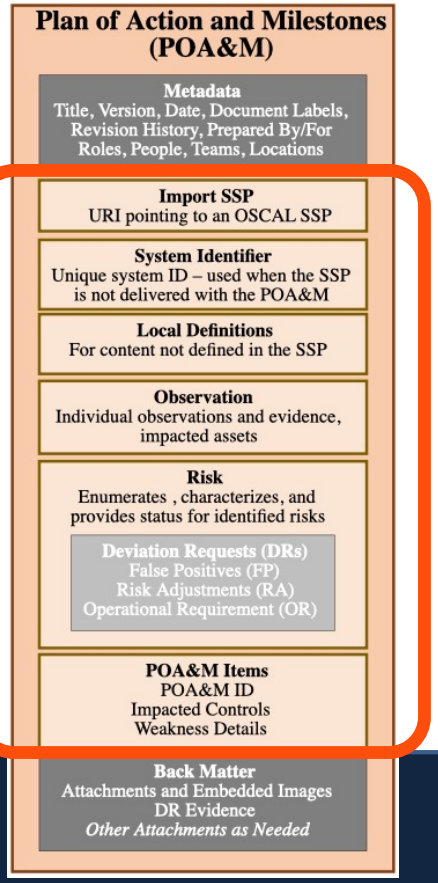
https://pages.nist.gov/OSCAL/reference/latest/plan-of-action-and-milestones/json-outline/

Plan of Action and Milestones Model v1.0.4 JSON Format Outline

The following outline is a representation of the JSON format for this model. For each property, the name links to the corresponding entry in the JSON Format Reference. The cardinality and data type are also provided for each property where appropriate.

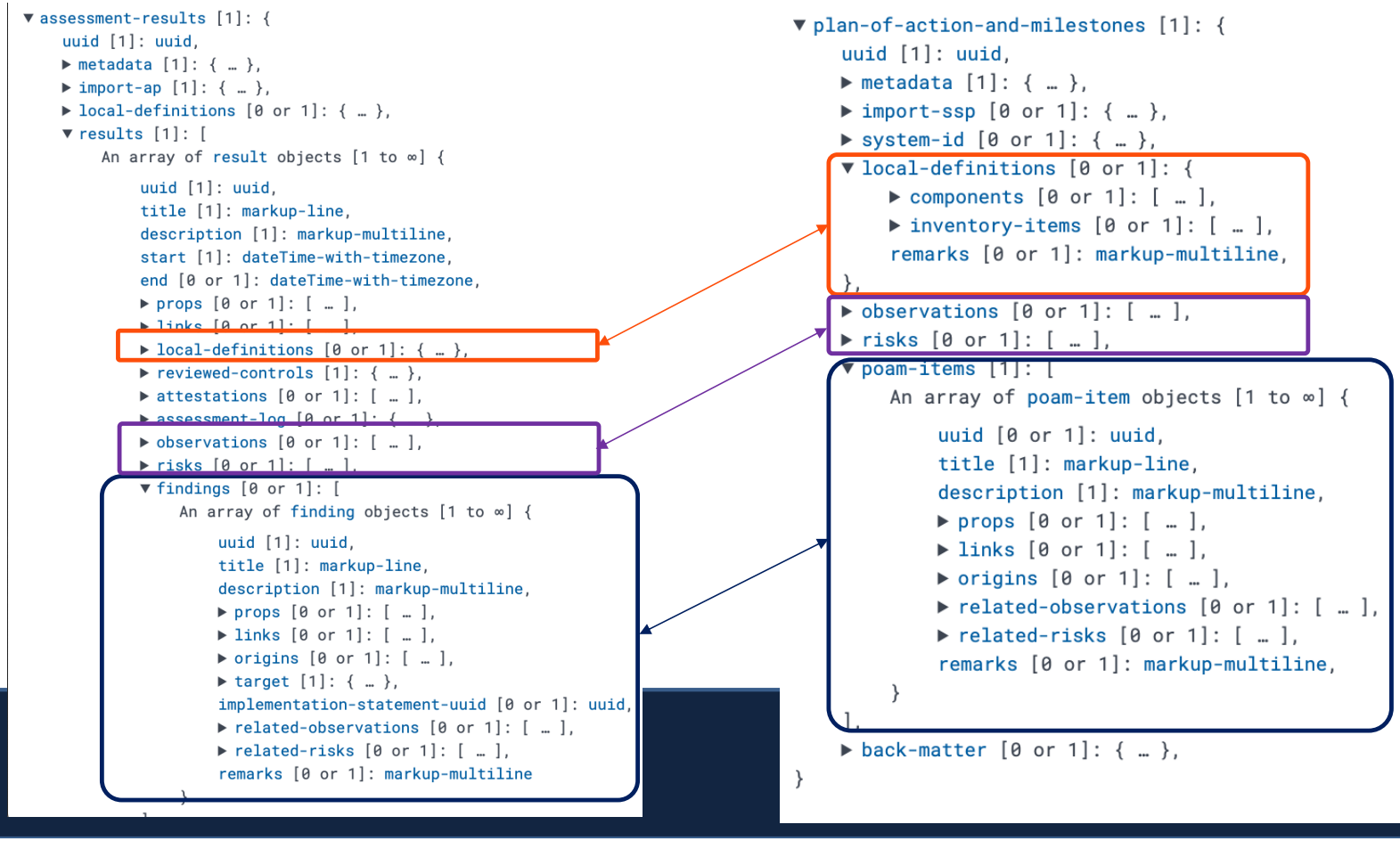
```
▼ plan-of-action-and-milestones [1]: {
    uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-ssp [0 or 1]: { … },
    ▶ system-id [0 or 1]: { … },
    ▶ local-definitions [0 or 1]: { … },
    ▶ observations [0 or 1]: [ … ],
    ▶ risks [0 or 1]: [ … ],
    ▶ poam-items [1]: [ … ],
    ▶ back-matter [0 or 1]: { … },
}
```

Root Element & Root UUID



The Assessment Results Model vs the POA&M Model

https://pages.nist.gov/OSCAL/reference/latest/plan-of-action-and-milestones/json-outline/



Thank you!

OSCAL is a community-driven program!

Please join us!

OSCAL Catalog Tutorial:
https://pages.nist.gov/OSCAL/learn/tutorials/control/basic-catalog/

https://www.nist.gov/OSCAL

Contact us at: oscal@nist.gov

Subscribe to our mailing lists: oscal-dev@list.nist.gov or oscal-updates@list.nist.gov

Chat with us on Gitter: https://gitter.im/usnistgov-OSCAL/Lobby

Collaborate with us on GitHub: https://github.com/usnistgov/OSCAL

Join our COI meetings: https://pages.nist.gov/OSCAL/contribute/#community-meetings