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 Layers

- **Controls Layer**
  - IMPORT CATALOG
  - OSCAL Catalog Model
  - ASSOCIATED PROFILES

- **Profile Model**
  - IMPORT PROFILE
  - OSCAL Profile Model

- **Implementation Layer**
  - IMPORT SSP
  - Component Definition Model

- **Assessment Layer**
  - IMPORT AP
  - OSCAL SSP Model
  - Components
  - ASSOCIATED PROFILES

  - OSCAL Assessment Plan Model
  - OSCAL Plan of Action and Milestones Model

  - OSCAL Assessment Results Model
  - OPEN RISKS
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.
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.
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

OSCAL Content

- Generation
- in Action

OSCAL Editorial Tools

OSCAL GRC Tools

https://github.com/usnistgov/OSCAL
https://github.com/usnistgov/oscal-content
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: the Open Security Controls Assessment Language

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


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 component definition, the cardinality and data type are also provided for each element or attribute.

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 element or component definition, the cardinality and data type are also provided for each property where applicable.
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 part, please refer to the JSON Format Reference. The cardinality and data type are also provided for each property where appropriate.

```json
• 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]: { ... },
}
```
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.

```json
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


assessment-plan

Security Assessment Plan (SAP)

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

  - **Properties (10)**

    - **uuid**
      - **uuid**
      - 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)**

      - Publication metadata

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

- **Switch to XML**
The Anatomy of the Assessment Plan - Body


```json
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]: { ... }
}
```

---

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

**Tasks**
- Scheduled events or milestones associated with a series of assessment actions. Timing, Dependencies, Associated activities, Subjects, Responsible roles.
The import statement. Imported content is what OSCAL content is linked as a result of.

```json
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


```json
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


```json
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

The Anatomy of the Assessment Plan – **Assessment Subject**

The Anatomy of the Assessment Plan – **Assessment Assets**


```
- 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


```json
  ▼ tasks [0 or 1]:
  /// An array of task objects [1 to ∞] {
    uid [1]: uid,
    title [1]: token,
    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]: uid,
      ▼ props [0 or 1]: [ … ],
      ▼ links [0 or 1]: [ … ],
      ▼ responsible-roles [0 or 1]: [ … ],
      ▼ subjects [0 or 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
```
The Anatomy of the Assessment Results Model – Body


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.

```json
  ▼ 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


Root Element & Root UUID

```json
assessment-results [1]: {
    uuid [1]: uuid,
    metadata [1]: { ... },
    import-ap [1]: { ... },
    local-defineds [0 or 1]: { ... },
    results [1]: [ ... ],
    back-matter [0 or 1]: { ... }
}
```
The Anatomy of the Assessment Results Model – Body

The Anatomy of the Assessment Results Model – Results
The Anatomy of the Assessment Results Model – Results

The Anatomy of the POA&M Model – the Body


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 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.

```json
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]: { ... },
}
```
The Assessment Results Model vs the POA&M Model

Thank you!

OSCAL is a community-driven program! Please join us!

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

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

https://www.nist.gov/OSCAL