



# Actions Beyond Words:

## Automating Audits for Streamlined Cybersecurity Compliance in Europe

**NIST** NATIONAL INSTITUTE OF  
STANDARDS AND TECHNOLOGY  
U.S. DEPARTMENT OF COMMERCE

# Continuous Proactive Security with OSCAL

Going Beyond 'Shifting Left Security'

**Dr. Michaela Iorga**  
Director, OSCAL Program  
ITL/NIST

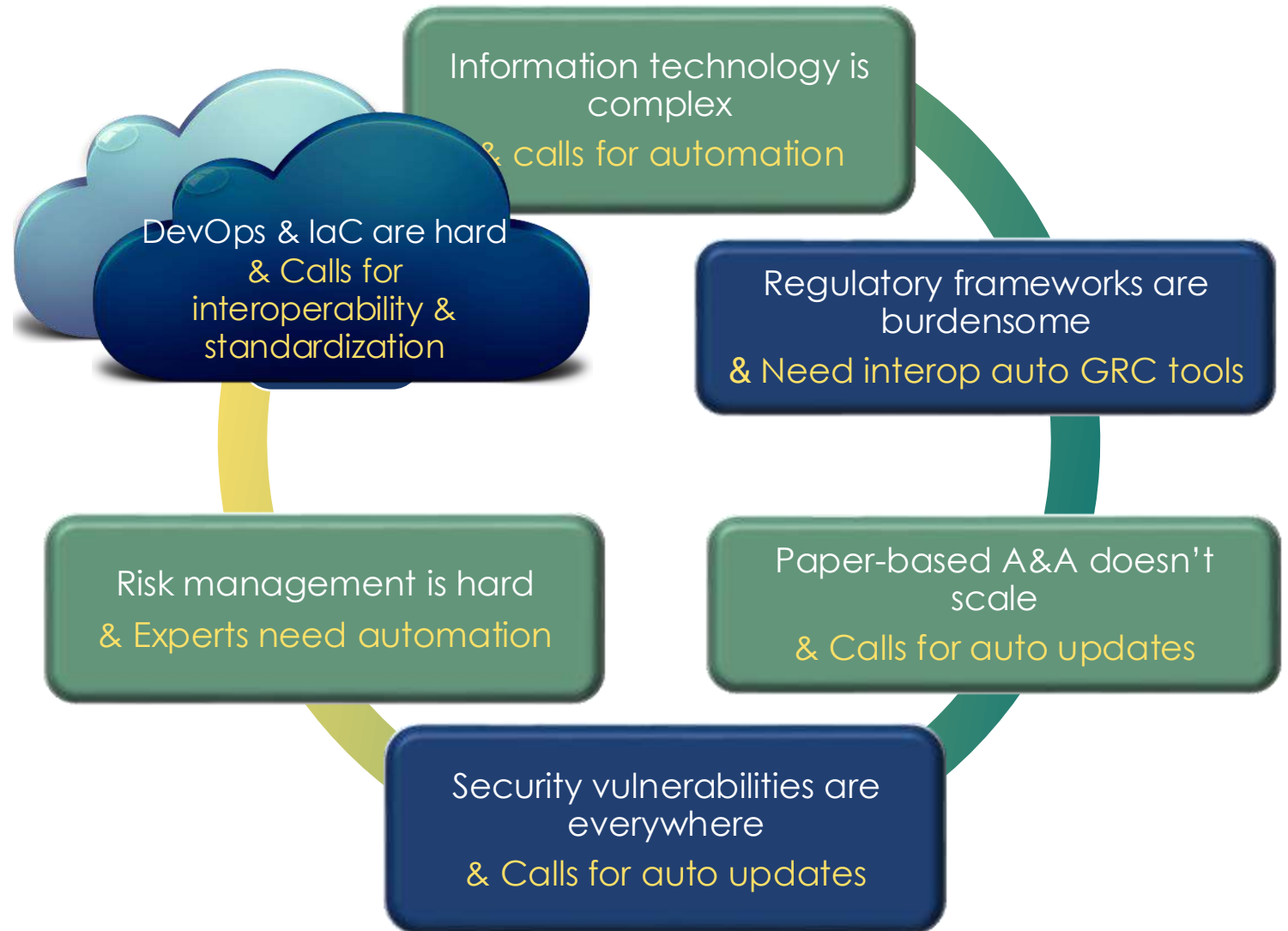
# Agenda

- ❑ Why NIST started OSCAL
- ❑ What is OSCAL
  - ❑ Released Models
  - ❑ Prototype Models
- ❑ Proactive security with OSCAL



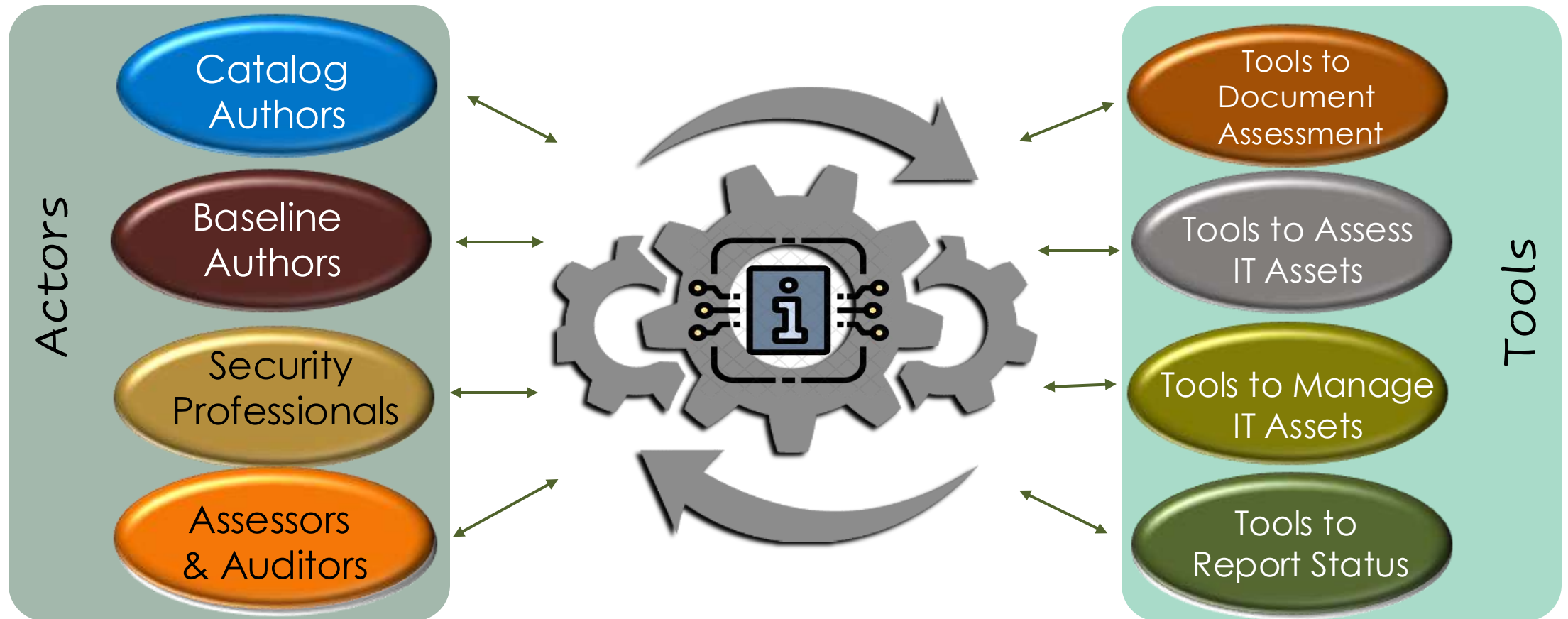


# The Problem ...



# The Solution ...

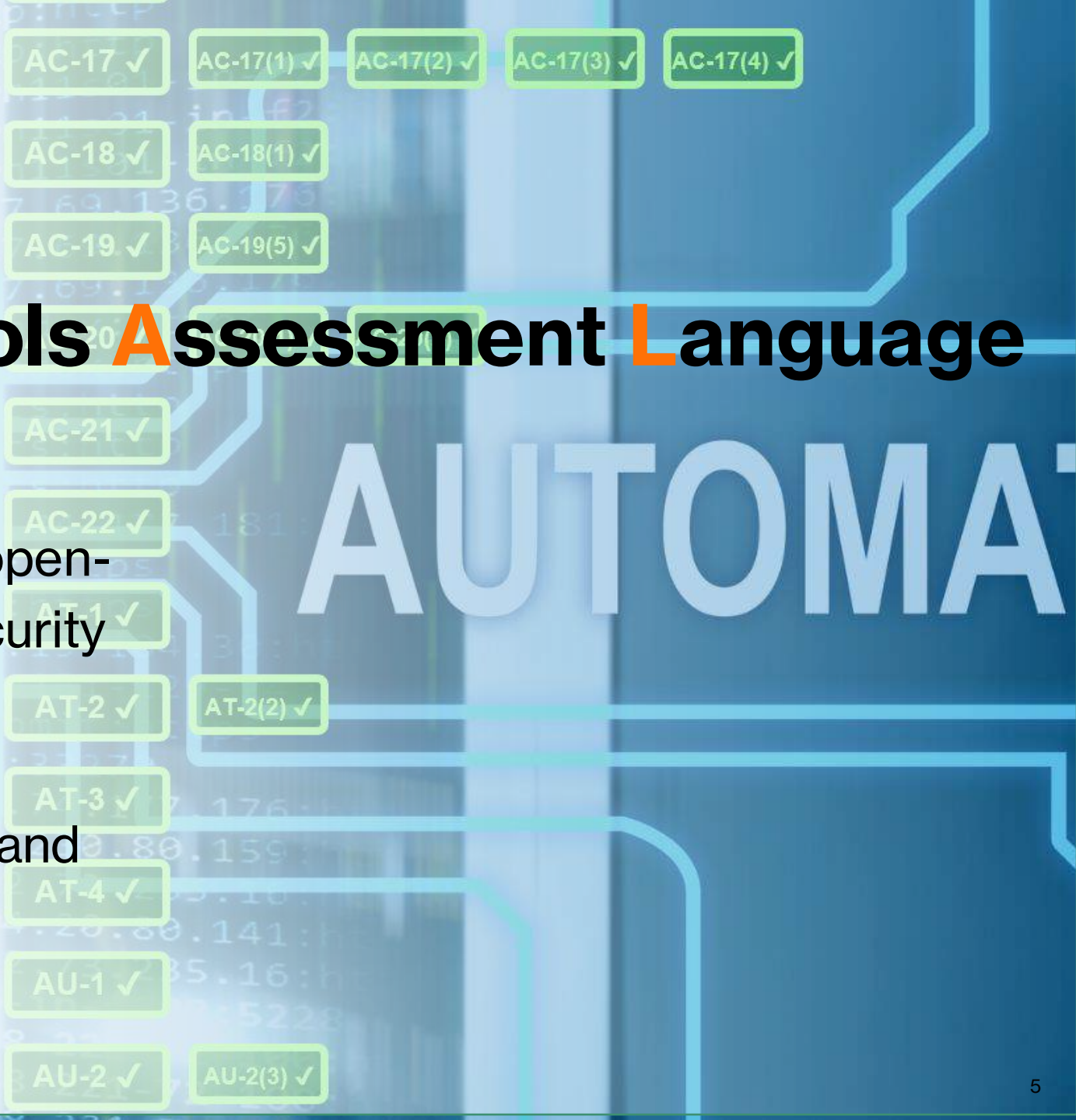
A (Cyber) Machine-readable Esperanto that enables actors, tools and organizations to exchange information via automation:



# The Implementation ...

## Open Security Controls Assessment Language

**OSCAL** is a standardized, flexible, open-source language that expresses security controls and their associated implementations and assessment methods in both, machine-readable and human formats.

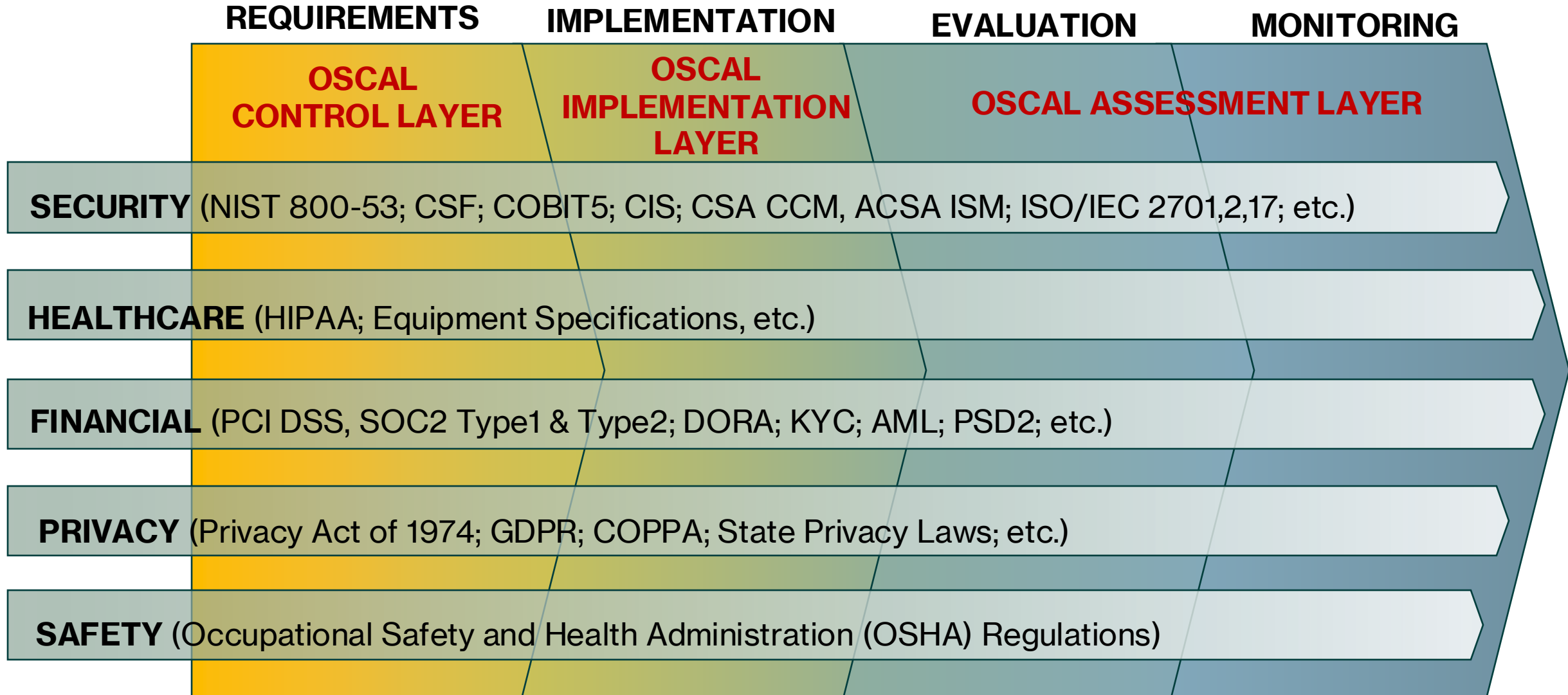


# Design Goals ...

- ❑ Improve the efficiency, timeliness, accuracy, and consistency of system security assessments
  - ❑ Enable traceability of design, implementation, and assessment back to the original control statements
  - ❑ Set the foundation for automation and interoperability
- 
- |              |  |
|--------------|--|
| ❑ Open       | ❑ Free for everyone  |
| ❑ Security   | ❑ Compliance (security, privacy, safety, etc...)                                     |
| ❑ Controls   | ❑ Requirements that needs assessment   |
| ❑ Assessment | ❑ Evaluation of the safeguard implemented in response of a set of requirements       |
| ❑ Language   | ❑ Digital representation – a translation of the information for machines to consume. |



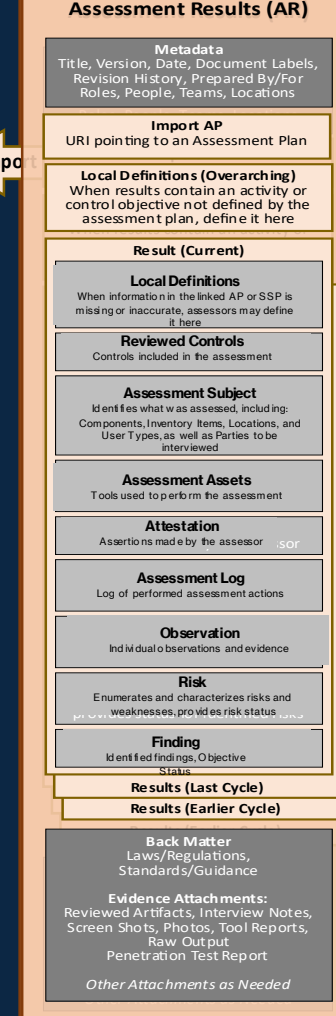
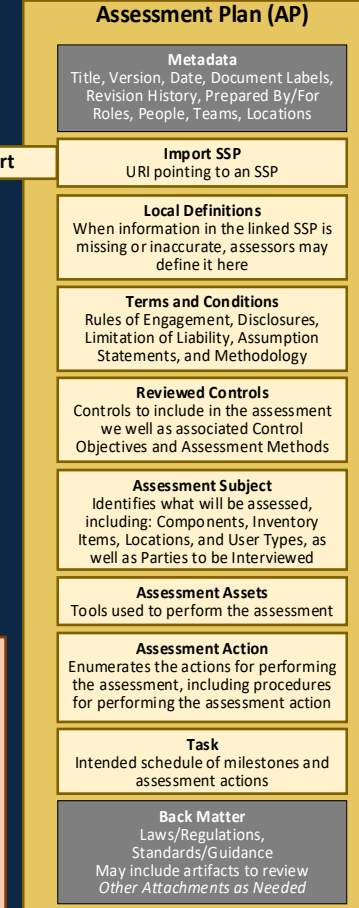
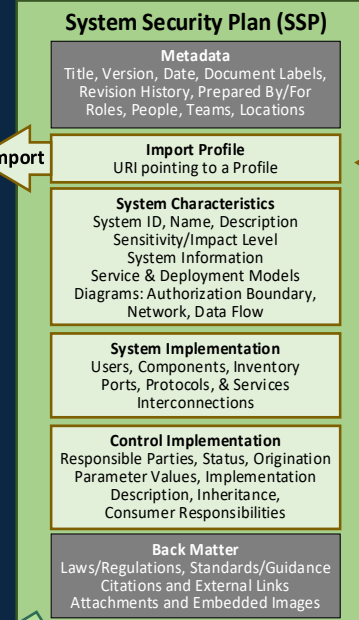
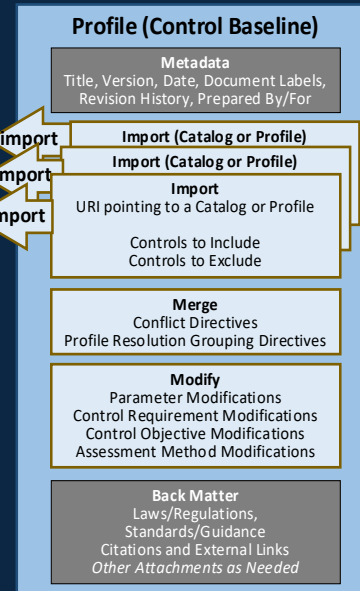
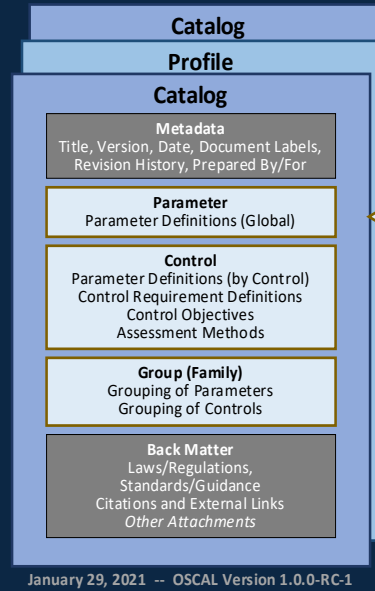
# Applicable to Any Domain ...



# CATALOG MODEL

# PROFILE MODEL

# SSP MODEL

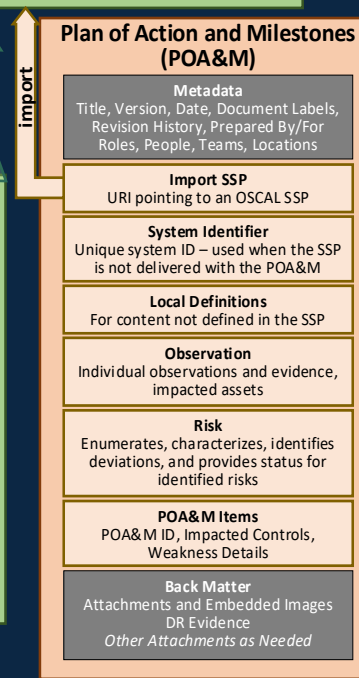
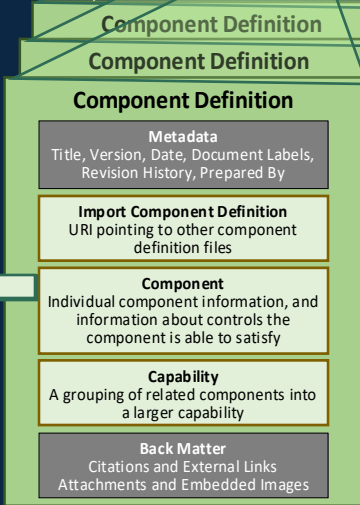


The **import** arrow identifies what OSCAL content is linked as a result of the import statement. Imported content referenced, not copied.

Associates configuration settings with baselines

Associates configuration settings with baselines

Transfers relevant content



## ASSESSMENT PLAN MODEL

## ASSESSMENT RESULTS MODEL

# OSCAL v1.1.3 Models

## COMPONENT MODEL

## POA&M MODEL



https://nist.gov/oscal



# OSCAL: the Open Security Controls Assessment Language

[Get involved](#) | [Contact Us](#) | [Github](#)

[About](#) | [Learn](#) | [Concepts](#) | [Reference](#) | [Downloads](#) | [Tools](#) | [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 ✓



**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.

# OSCAL Models' 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 corresponding entry in the [XML Format Reference](#). The cardinality and data type are also provided for each element or attribute within the XML schema.

```
<?xml version="1.0" encoding="UTF-8" ?>
<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]
```

**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

## 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 in the [JSON Format Reference](#). The cardinality and data type are also provided for each property where appropriate.

```
{
  "catalog": {
    "uuid": "uuid",
    "metadata": {
      "type": "string"
    },
    "params": [
      {
        "id": "token",
        "class": "token",
        "depends-on": "token"
      }
    ],
    "controls": [
      {
        "id": "token",
        "class": "token"
      }
    ],
    "groups": [
      {
        "id": "token",
        "class": "token"
      }
    ],
    "back-matter": {
      "type": "string"
    }
  },
  "profile": {
    "uuid": "uuid",
    "metadata": {
      "type": "string"
    },
    "imports": [
      {
        "href": "uri-reference"
      }
    ],
    "merge": {
      "type": "string"
    },
    "modify": {
      "type": "string"
    },
    "back-matter": {
      "type": "string"
    }
  },
  "component-definition": {
    "uuid": "uuid",
    "metadata": {
      "type": "string"
    },
    "import-component-definitions": [
      {
        "href": "uri-reference"
      }
    ],
    "components": [
      {
        "uuid": "uuid",
        "type": "string"
      }
    ],
    "capabilities": [
      {
        "uuid": "uuid",
        "name": "string"
      }
    ],
    "back-matter": {
      "type": "string"
    }
  },
  "system-security-plan": {
    "uuid": "uuid",
    "metadata": {
      "type": "string"
    },
    "import-profile": {
      "href": "uri-reference"
    },
    "system-characteristics": {
      "type": "string"
    },
    "system-implementation": {
      "type": "string"
    },
    "control-implementation": {
      "type": "string"
    },
    "back-matter": {
      "type": "string"
    }
  },
  "assessment-plan": {
    "uuid": "uuid"
  },
  "assessment-results": {
    "uuid": "uuid"
  },
  "plan-of-action-and-milestones": {
    "uuid": "uuid"
  }
}
```



# OSCAL Models' References

OSCAL Complete v1.0.4 XML Format Reference

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 v1.1 XML Format Reference

The following is the XML format reference for the combination of all OSCAL models, which is organized hierarchically. Each entry represents the corresponding XML element or attribute in the model's XML format, and provides details about the semantics and use of the element or attribute. The [XML Format Outline](#) provides a streamlined, hierarchical representation of this model's XML format which can be used along with this reference to better understand the XML representation of this model.

**XML NAMESPACE** <http://csrc.nist.gov/ns/oscal/1.0>

This format represents a combination of all of the OSCAL models.

**catalog** element (global definition) [Switch to JSON](#)

Catalog

**DESCRIPTION** A collection of controls.

▼ Remarks

Catalogs may use one or more **group** objects to subdivide the control contents of a catalog.

An OSCAL catalog model provides a structured representation of control information.

▼ Constraints (2)

**ALLOWED VALUE** for `metadata/prop[has-oscal-namespace('http://csrc.nist.gov/ns/oscal')]/@name`

The value **must** be one of the following:

- resolution-tool**: The tool used to produce a resolved profile.

**ALLOWED VALUE** for `metadata/link/@rel`

The value **must** be one of the following:

- source-profile**: The tool used to produce a resolved profile.

▼ Attribute (1)

**uuid** uuid [1] [Switch to JSON](#)

Catalog Universally Unique Identifier

**DESCRIPTION** A globally unique identifier with cross-instance scope for this catalog instance. This UUID should be changed when this document is revised.

▼ Elements (5)

**metadata** element (global definition) [1] [Switch to JSON](#)

OSCAL Complete v1.0.4 JSON Format Reference

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 v1.1 JSON Format Reference

The following is the JSON format reference for the combination of all OSCAL models, which is organized hierarchically. Each entry represents the corresponding JSON property in the model's JSON format, and provides details about the semantics and use of the property. The [JSON Format Outline](#) provides a streamlined, hierarchical representation of this model's JSON format which can be used along with this reference to better understand the JSON representation of this model.

**JSON BASE URI** <http://csrc.nist.gov/ns/oscal/1.0>

This format represents a combination of all of the OSCAL models.

**catalog** object (global definition) [Switch to XML](#)

Catalog

**DESCRIPTION** A collection of controls.

▼ Remarks

Catalogs may use one or more **group** objects to subdivide the control contents of a catalog.

An OSCAL catalog model provides a structured representation of control information.

▼ Constraints (2)

**ALLOWED VALUE** for `metadata/prop[has-oscal-namespace('http://csrc.nist.gov/ns/oscal')]/@name`

The value **must** be one of the following:

- resolution-tool**: The tool used to produce a resolved profile.

**ALLOWED VALUE** for `metadata/link/@rel`

The value **must** be one of the following:

- source-profile**: The tool used to produce a resolved profile.

▼ Properties (6)

**uuid** uuid [1] [Switch to XML](#)

Catalog Universally Unique Identifier

**DESCRIPTION** A globally unique identifier with cross-instance scope for this catalog instance. This UUID should be changed when this document is revised.

**metadata** object (global definition) [1] [Switch to XML](#)

# OSCAL Releases ...



FIRST OSCAL 1.0.0

RELEASED ON JUNE 7, 2021

LATEST: OSCAL 1.1.3



<https://github.com/usnistgov/OSCAL/releases>

*"...First official, major release of OSCAL provides a stable OSCAL 1.0.0 for wide-scale implementation ..."*

*Latest OSCAL patch release : 1.1.3 - backwards compatible.*




# OSCAL Ecosystem

```
▼ 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-profiles [0 or 1]: { - },
  ▶ system-changes [0 or 1]: { - },
  ▶ control-implementation [1]: { - },
  ▶ back-matter [0 or 1]: { - },
},
▼ 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]: { - },
},
▼ assessment-results [1]: {
  uuid [1]: uuid,
  ▶ metadata [1]: { - },
  ▶ import-asp [1]: { - },
  ▶ local-definitions [0 or 1]: { - },
  ▶ results [1]: { - },
  ▶ back-matter [0 or 1]: { - },
},
▼ 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]: { - },
},
}
```

OSCAL Models

<https://github.com/usnistgov/OSCAL>



usnistgov / oscal-content Public

<> Code Issues 22 Pull requests 2

master oscal-content / nist.gov / SP800-53 / rev5 / xml /

Download under Polishing and converted... 03 Apr 27

draft

- NIST\_SP-800-53\_rev5\_HIGH-baseline-resolved-profile...
- NIST\_SP-800-53\_rev5\_LOW-baseline-resolved-profile...
- NIST\_SP-800-53\_rev5\_MODERATE-baseline-resolved-...
- NIST\_SP-800-53\_rev5\_PRIVACY-baseline-resolved-pr...
- NIST\_SP-800-53\_rev5\_catalog.xml

OSCAL Content Generation

OSCAL Content in Action

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

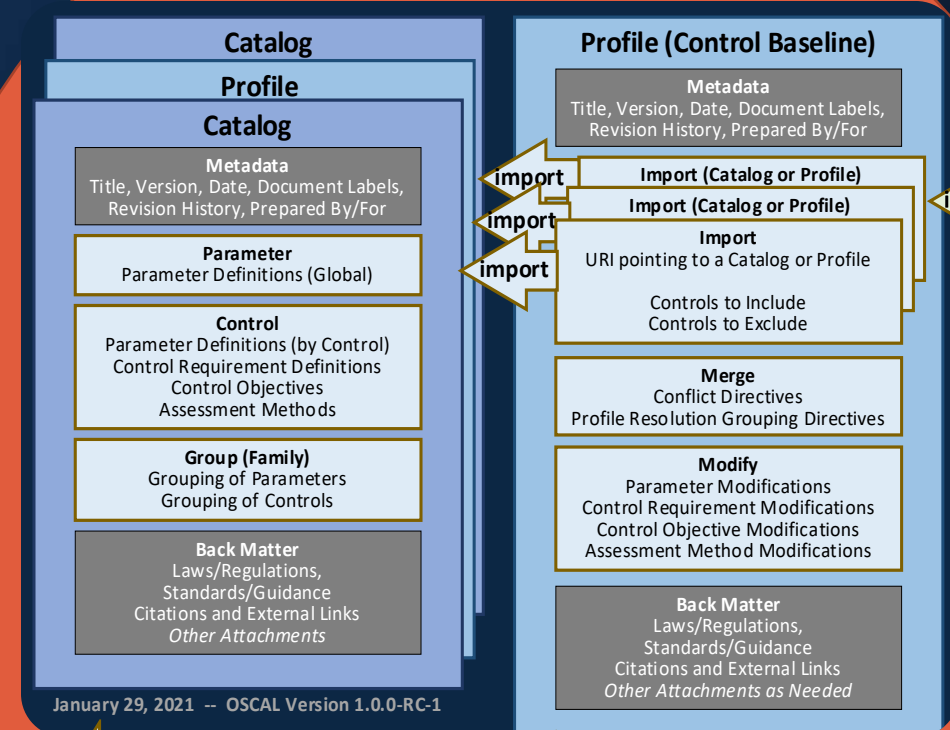
Name	Provider/Developer	Description	Type
<a href="#">Compliance trestle</a>	IBM	A python SDK and command line tool which manipulates OSCAL structures and supports transformation of data into OSCAL.	open source
<a href="#">OSCAL Java Library</a>	NIST OSCAL Project	A Java-based programming API for reading and writing content conformant to the OSCAL XML, JSON, and YAML based models.	open source
<a href="#">OSCAL React Component Library</a>	Easy Dynamics	A library of reusable React components and an <a href="#">example user interface application</a> that provides a direct UI into OSCAL.	open source
<a href="#">OSCAL React API</a>		An <a href="#">example application</a> that provides a direct UI into OSCAL. It uses the OSCAL React API to read and write OSCAL content and provides system change manipulation, catalogs, profiles, components, and SSPs.	open source
<a href="#">XSLT Tooling</a>	NIST OSCAL Project	A variety of <a href="#">Example Stylesheet</a> (XSLT) transformations for OSCAL content, including XSLT for XSLT, and related utilities for authoring, converting, and publishing OSCAL content in various forms.	open source
<a href="#">XML Jelly Sandwich</a>	Wendell Piez (NIST)	Interactive XSLT in the browser includes <a href="#">OSCAL demonstrations</a> .	open source
<a href="#">Xacta 360</a>		Xacta 360 is a cyber risk management and compliance platform that enables users to create and submit OSCAL content and supports OSCAL system security plans (SSPs) in OSCAL format. Future OSCAL capabilities are forthcoming as the tool evolves.	license
<a href="#">Atlasity: Continuous Compliance Automation</a>	C2 Labs	Atlasity (referred to as Atlasity) runs in any environment and supports the development of OSCAL v1.0 content for Catalogs, Profiles, System Security Plans and Components. Additional detail can be found in this <a href="#">blog post: Atlasity Delivers Free Tools to Create OSCAL Content</a> .	community edition

OSCAL Editorial Tools

OSCAL GRC Tools

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

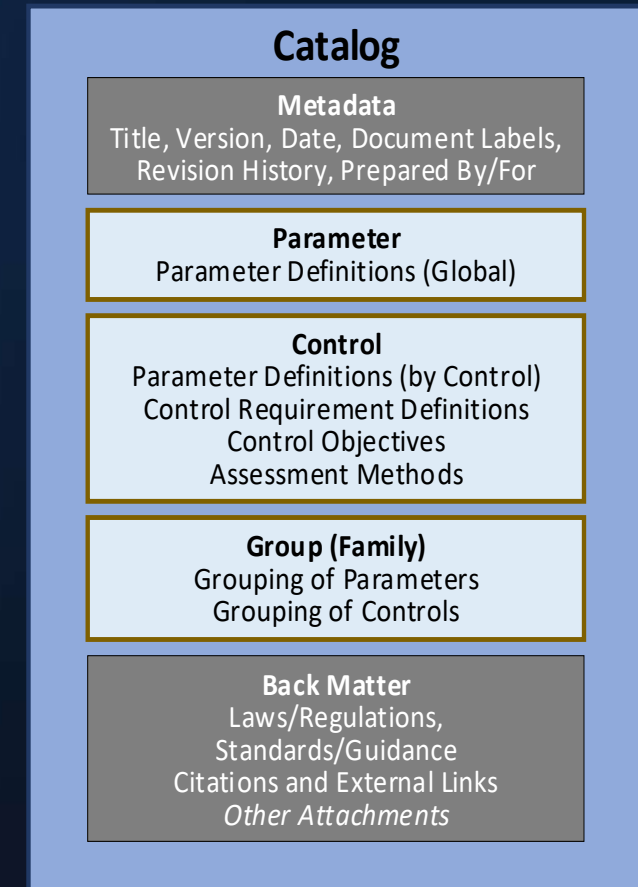
# OSCAL Controls Layer



# OSCAL Catalog Model

**Represents a collection of security and privacy controls, which may be used as part of a risk management program.**

- **Metadata:** Same for each OSCAL model
- **Parameter:** Provides a global policy variable used by one or more control
- **Control:** An individual control in the catalog.
  - May contain control-specific parameters, control requirement statements, control objectives, assessment methods, references
  - Controls can have child controls.
- **Group:** Related controls may be grouped. Parameters related to this group may be defined here.
- **Back Matter:** Same for each OSCAL model



# OSCAL

## Catalog Model

### 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*

```
▼ <catalog uuid="uuid"> [1]
  ▶ <metadata> ... </metadata> [1]
  ▶ <param id="token" class="token" depends-on="token"> ... </param> [0 to ∞]
  ▼ <control id="token" class="token"> [0 to ∞]
    ▶ <title>markup-line</title> [1]
    ▶ <param id="token" class="token" depends-on="token"> ... </param> [0 to ∞]
    ▶ <prop name="token" uuid="uuid" ns="uri" value="string" class="token" group="token">
      ... </prop> [0 to ∞]
    ▶ <link href="uri-reference" rel="token" media-type="string" resource-
      fragment="string"> ... </link> [0 to ∞]
    ▶ <part id="token" name="token" ns="uri" class="token"> ... </part> [0 to ∞]
      <control> (recursive: model like parent control) </control> [0 to ∞]
    </control>
  ▼ <group id="token" class="token"> [0 to ∞]
    ▶ <title>markup-line</title> [1]
    ▶ <param id="token" class="token" depends-on="token"> ... </param> [0 to ∞]
    ▶ <prop name="token" uuid="uuid" ns="uri" value="string" class="token" group="token">
      ... </prop> [0 to ∞]
    ▶ <link href="uri-reference" rel="token" media-type="string" resource-
      fragment="string"> ... </link> [0 to ∞]
    ▶ <part id="token" name="token" ns="uri" class="token"> ... </part> [0 to ∞]
      A choice of:
      <group> (recursive: model like ancestor group) </group> [0 to ∞]
      ▶ <control id="token" class="token"> ... </control> [0 to ∞]
    </group>
  ▶ <back-matter> ... </back-matter> [0 or 1]
</catalog>
```



# OSCAL Profile Model

**Used to establish a baseline of controls to be implemented with a system.**

➤ **Metadata:** Same for each OSCAL model

➤ **Import:** Identifies an OSCAL catalog or other profile to import controls from

- A control must be imported to be included in a baseline.
- All parameters and back-matter resources cited by an imported control are also imported.

➤ **Merge:** Provides directives used to organize controls and to resolve conflicts when the same control is imported multiple times

➤ **Modify:** Allows tailoring of imported controls, including their parameters, control requirement definitions, references, control objectives, and assessment actions.

➤ **Back Matter:** Same for each OSCAL model

## 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

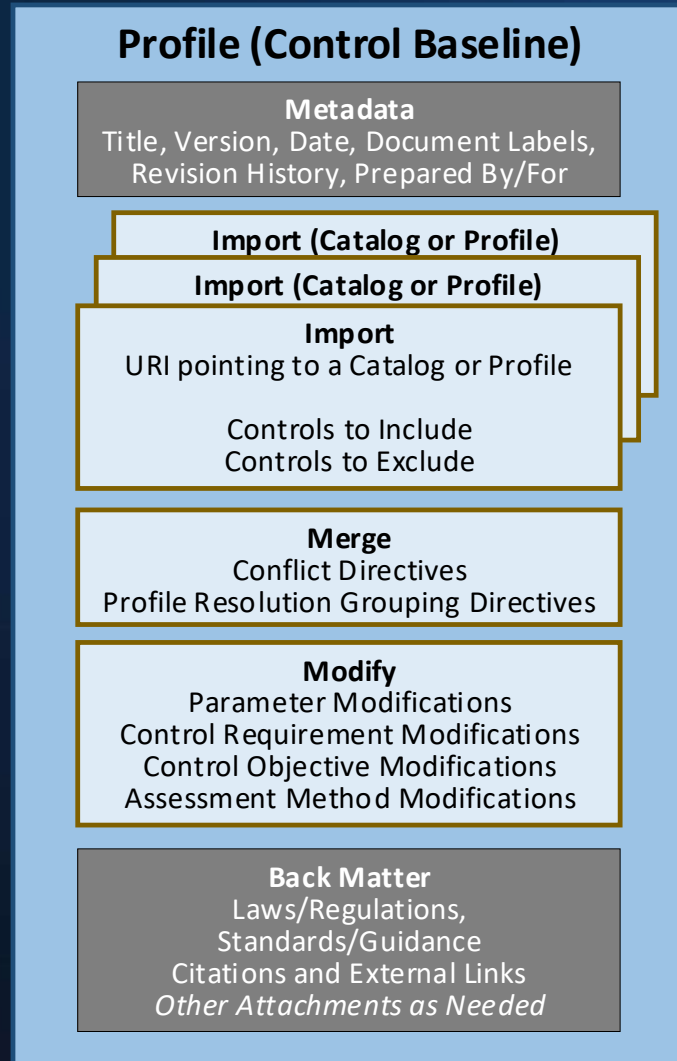
### Modify

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*

# OSCAL Profile Model



Each element of an instance where appropriate:

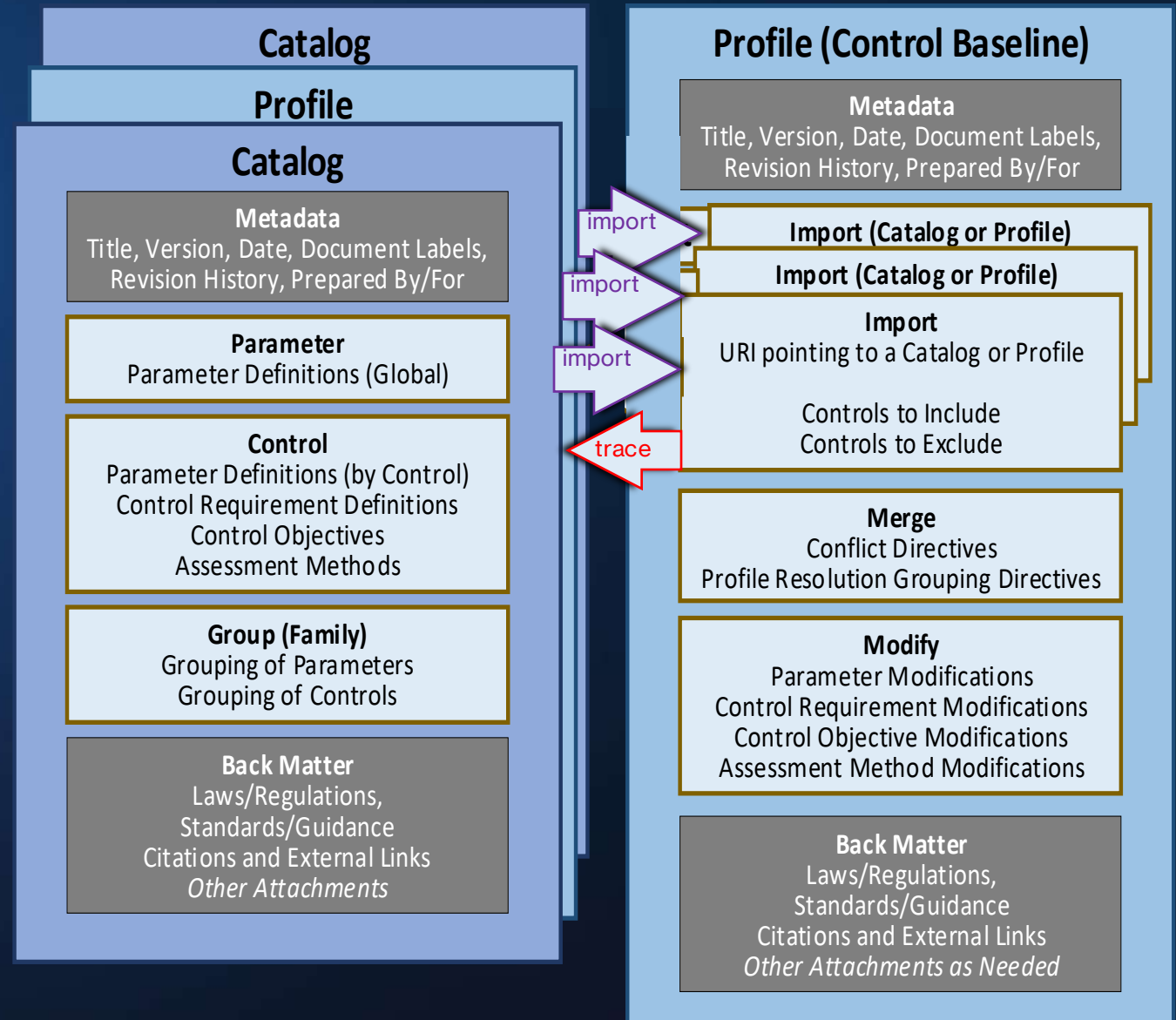
```
<profile uuid="uuid"> [1]
  <metadata> ... </metadata> [1]
  <import href="uri-reference"> [1 to ∞]
    A choice of:
    > <include-all/> [1]
    > <include-controls with-child-controls="token"> ... </include-controls> [1 to ∞]
    > <exclude-controls with-child-controls="token"> ... </exclude-controls> [0 to ∞]
  </import>
  <merge> [0 or 1]
    > <combine method="string"/> [0 or 1]
    A choice of:
    > <flat/> [1]
    > <as-is>boolean</as-is> [1]
    > <custom> ... </custom> [1]
  </merge>
  <modify> [0 or 1]
    > <set-parameter param-id="token" class="token" depends-on="token"> ... </set-parameter>
      [0 to ∞]
    > <alter control-id="token"> ... </alter> [0 to ∞]
  </modify>
  > <back-matter> ... </back-matter> [0 or 1]
</profile>
```

# OSCAL Profile Model – Native Traceability

A profile can import controls from:

- A catalog or multiple catalogs
- Another profile or multiple profiles

This allows a baseline to be established by customizing another baseline.



# EXAMPLE: A 27002 CONTROL (PROSE)

## 6.1.2 Segregation of duties

### Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

### Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls. Small organizations may find segregation of duties difficult to achieve, but the principle should be

applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

### Other information

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.



# EXAMPLE OSCAL XML CATALOG:

```
</control>
<control class="ssc-iso-sc27" id="s6.1.2">
  <title>Segregation of duties</title>
  <prop name="label">6.1.2</prop>
  <prop name="sort-id">c02</prop>
  <part id="s6.1.2_stm" name="statement">
    <prop name="label">Control</prop>
    <p>Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.</p>
  </part>
  <part id="s6.1.2_gdn" name="guidance">
    <prop name="label">Implementation guidance</prop>
    <part id="s6.1.2_gdn.1" name="guidance">
      <p>Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.</p>
    </part>
    <part id="s6.1.2_gdn.2" name="guidance">
      <p>Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.</p>
    </part>
  </part>
  <part id="s6.1.2_inf" name="information">
    <prop name="label">Other information</prop>
    <p>Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.</p>
  </part>
</control>
```

# EXAMPLE OSCAL JSON CATALOG:

```
{
  "id" : "s6.1.2",
  "title" : "Segregation of duties",
  "properties" : [ {
    "name" : "label",
    "value" : "6.1.2"
  } ],
  "parts" : [ {
    "id" : "s6.1.2_stm",
    "name" : "statement",
    "title" : "Control",
    "prose" : "Conflicting duties and areas of responsibility should be\n segregated to reduce opportunities for unauthorized or unintentional\n modification or misuse of the organization's assets."
  }, {
    "id" : "s6.1.2_gdn",
    "name" : "guidance",
    "title" : "Implementation Guidance"
    "parts" : [ {
      "id" : "s6.1.2_gdn.1",
      "name" : "item",
      "prose" : "Care should be taken that no single person can access,\n modify or use assets without authorization or detection. \n\n The initiation of an event should be separated from its\n authorization. The possibility of collusion should be\n considered in designing the controls."
    }, {
      "id" : "s6.1.2_gdn.2",
      "name" : "item",
      "prose" : "Small organizations may find segregation of duties\n difficult to achieve, but the principle should be applied\n as far as is possible and practicable. Whenever it is\n difficult to segregate, other controls such as monitoring\n of activities, audit trails and management supervision\n should be considered."
    } ]
  }, {
    "id" : "s6.1.2_inf",
    "name" : "information",
    "title" : "Other Information"
    "prose" : "Segregation of duties is a method for reducing the risk\n of accidental or deliberate misuse of an organization's\n assets."
  } ]
}
```

# EXAMPLE OSCAL YAML CATALOG:

```
- id: s6.1.2
  title: Segregation of duties
  properties:
  - name: label
    value: 6.1.2
  parts:
  - id: s6.1.2_stm
    name: statement
    title: Control
    prose: |-
      Conflicting duties and areas of responsibility should be segregated
      to reduce opportunities for unauthorized or unintentional
      modification or misuse of the organization's assets.
  - id: s1.1.2_gdn
    name: guidance
    title: Implementation guidance
    parts:
    - id: s1.1.2_gdn.1
      name: item
      prose: |-
        Care should be taken that no single person can access, modify or
        use assets without authorization or detection. The initiation of an
        event should be separated from its authorization. The possibility
        of collusion should be considered in designing the controls.
    - id: s1.1.2_gdn.2
      name: item
      prose: |-
        Small organizations may find segregation of duties difficult to
        achieve, but the principle should be applied as far as is possible
        and practicable. Whenever it is difficult to segregate, other
        controls such as monitoring of activities, audit trails and
        management supervision should be considered.
  - id: s1.1.2_inf
    name: information
    title: Other information
    prose: |-
      Segregation of duties is a method for reducing the risk of accidental
      or deliberate misuse of an organization's assets.
```



# Translate 27002 in OSCAL XML

## ENGLISH

```
</control>
<control class="ssc-iso-sc27" id="s6.1.2">
  <title>Segregation of duties</title>
  <prop name="label">6.1.2</prop>
  <prop name="sort-id">c02</prop>
  <part id="s6.1.2_stm" name="statement">
    <prop name="label">Control</prop>
    <p>Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.</p>
  </part>
  <part id="s6.1.2_gdn" name="guidance">
    <prop name="label">Implementation guidance</prop>
    <part id="s6.1.2_gdn.1" name="guidance">
      <p>Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.</p>
    </part>
    <part id="s6.1.2_gdn.2" name="guidance">
      <p>Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.</p>
    </part>
  </part>
  <part id="s6.1.2_inf" name="information">
    <prop name="label">Other information</prop>
    <p>Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.</p>
  </part>
</control>
```

## FRENCH

```
</control>
<control class="ssc-iso-sc27" id="s6.1.2">
  <title>Séparation des tâches</title>
  <prop name="label">6.1.2</prop>
  <prop name="sort-id">c02</prop>
  <part id="s6.1.2_stm" name="statement">
    <prop name="label">Mesure</prop>
    <p>Il convient de séparer les tâches et les domaines de responsabilité incompatibles pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.</p>
  </part>
  <part id="s6.1.2_gdn" name="guidance">
    <prop name="label">Préconisations de mise en oeuvre</prop>
    <part id="s6.1.2_gdn.1" name="guidance">
      <p>Il convient de veiller à ce que personne ne puisse accéder à, modifier ou utiliser des actifs sans en avoir reçu l'autorisation ou sans avoir été détecté. Il convient de séparer le déclenchement d'un événement de son autorisation. Il convient d'envisager la possibilité de collusion lors de la conception des mesures.</p>
    </part>
    <part id="s6.1.2_gdn.2" name="guidance">
      <p>Les organisations de petite taille peuvent avoir des difficultés à réaliser une séparation des tâches, mais il convient d'appliquer ce principe dans la mesure du possible. Lorsqu'il est difficile de procéder à la séparation des tâches, il convient d'envisager d'autres mesures comme la surveillance des activités, des systèmes de traçabilité et la supervision de la direction.</p>
    </part>
  </part>
  <part id="s6.1.2_inf" name="information">
    <prop name="label">Informations supplémentaires</prop>
    <p>La séparation des tâches est une méthode permettant de diminuer les risques de mauvais usage, accidentel ou délibéré, des actifs d'une organisation.</p>
  </part>
</control>
```



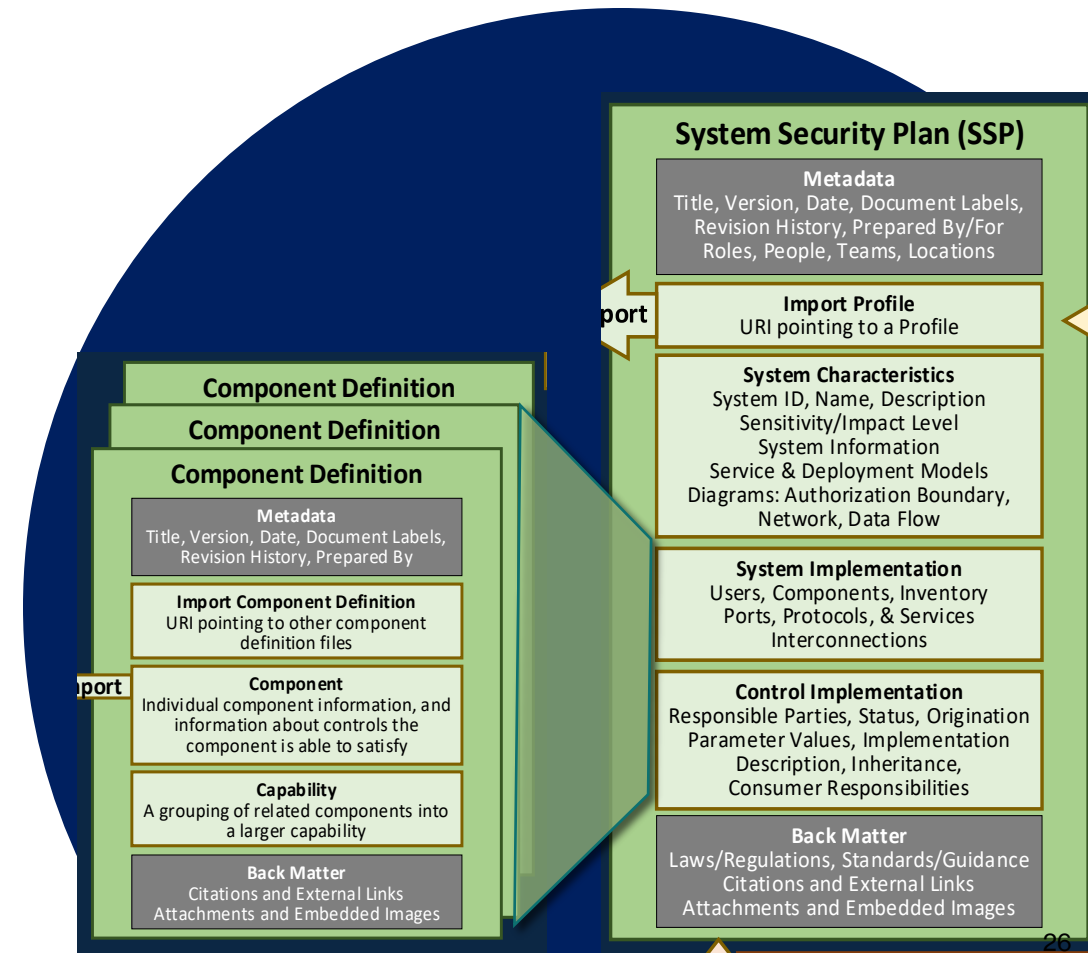
# OSCAL & Translations of 27002

- ❑ OSCAL minimizes the discrepancies between translated versions.
  - “*Other information*” and “*Informations supplémentaires*” will have the same tag
- ❑ OSCAL can support automatic translation of the standard (e.g dedicated tool).

# Shifting Left with OSCAL

## Implementation Layer

- ❑ Component Definition Model
- ❑ System Security Plan (SSP) Model



# The Component Definition ...

<https://pages.nist.gov/OSCAL/reference/latest/component-definition/>

Defines how the component or capability supports a set of controls.

```
▼ 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]: { ... },  
}
```

## 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 Component Definition

<https://pages.nist.gov/OSCAL/reference/latest/component-definition/>

```
▼ control-implementations [0 or 1] [
  An array of control-implementation objects [1 to ∞] {
    uuid [1]: uuid,
    source [1]: uri-reference,
    description [1]: markup-multiline,
    ▶ props [0 or 1]: [ ... ],
    ▶ links [0 or 1]: [ ... ],
    ▶ set-parameters [0 or 1]: [ ... ],
    ▼ implemented-requirements [1]: [
      An array of implemented-requirement objects [1 to ∞] {
        uuid [1]: uuid,
        control-id [1]: token,
        description [1]: markup-multiline,
        ▶ props [0 or 1]: [ ... ],
        ▶ links [0 or 1]: [ ... ],
        ▶ set-parameters [0 or 1]: [ ... ],
        ▶ responsible-roles [0 or 1]: [ ... ],
        ▶ statements [0 or 1]: [ ... ],
        remarks [0 or 1]: markup-multiline,
      }
    ],
  },
],
}
```

## 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

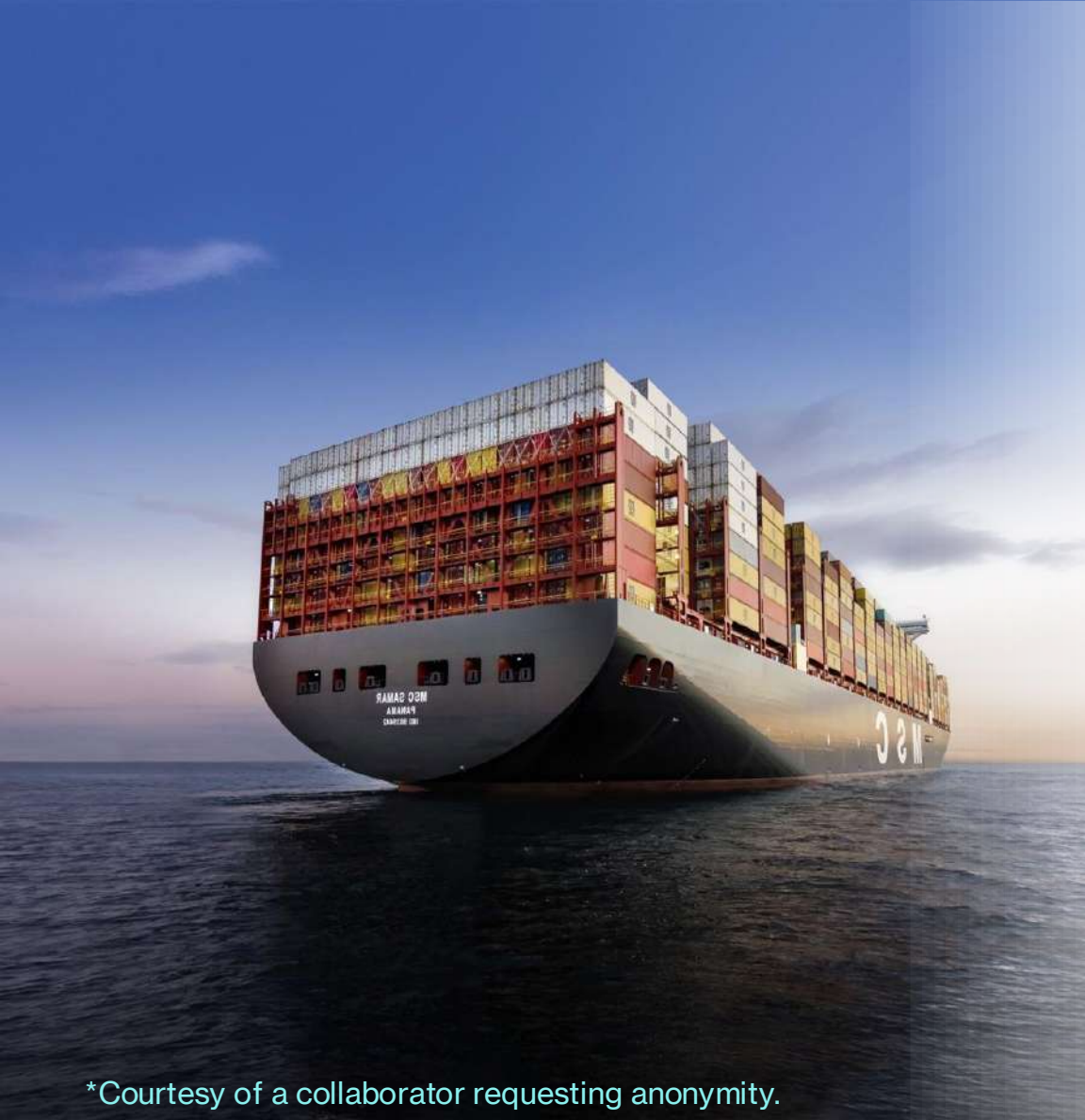
A grouping of related components into  
a larger capability

### Back Matter

Citations and External Links  
Attachments and Embedded Images



# Cybersecurity 'Shipping Container\*'



OSCAL Component Definition (Cdef) instances are like the maritime shipping containers!

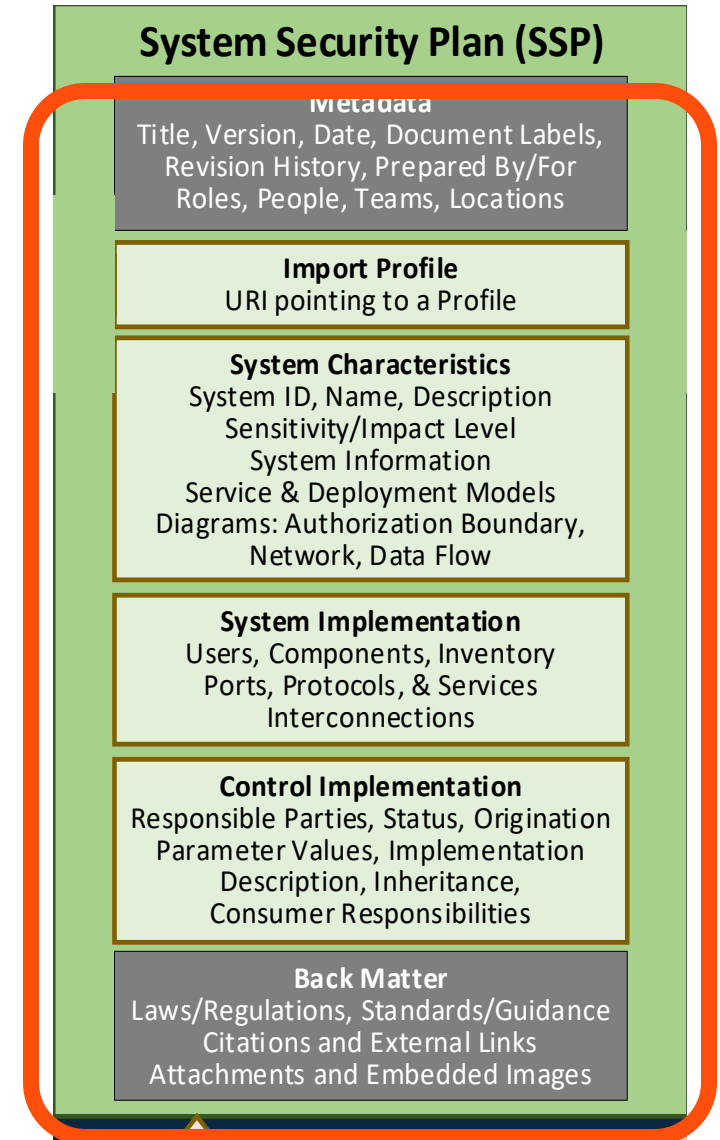
OSCAL Component Definition Model allows:

- ☐ Vendors to document the security controls implemented by their products
- ☐ System owners or policy makers to define 'playbooks' for system components
- ☐ System owners to test, review and provisionally authorize system components
- ☐ Reuse the components for different systems
- ☐ Ease the system's documentation generation
- ☐ Human-intensive labor of generating SSP to be semi-automated

# The SSP Model

<https://pages.nist.gov/OSCAL/reference/latest/system-security-plan/json-outline/>

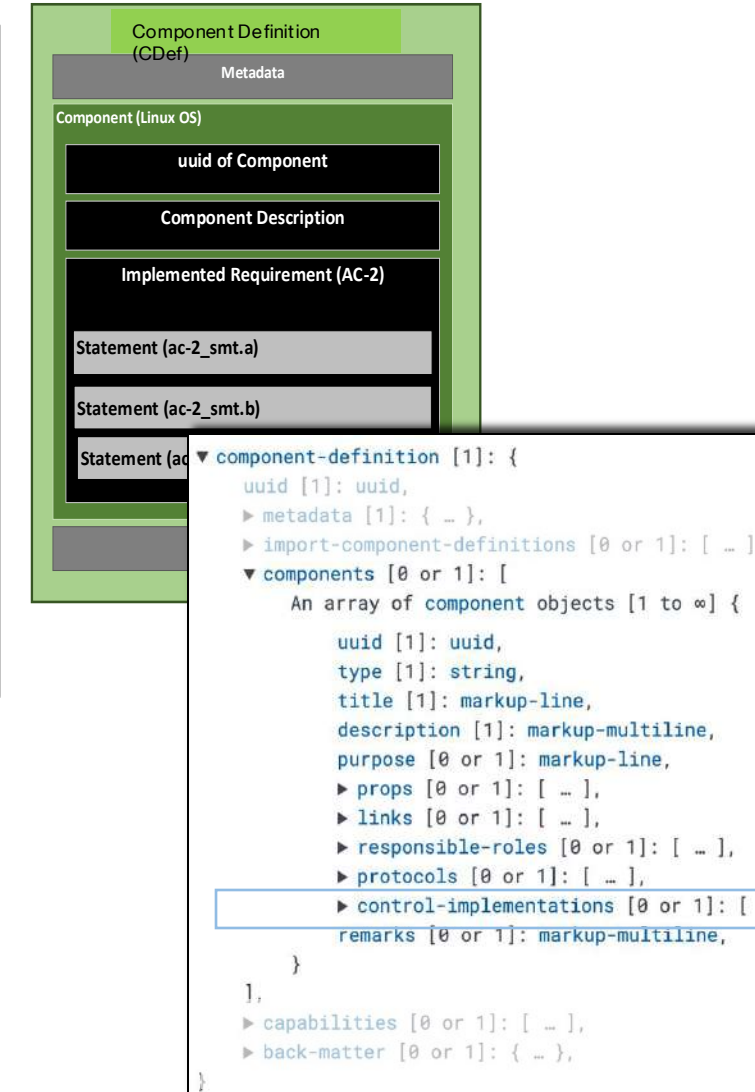
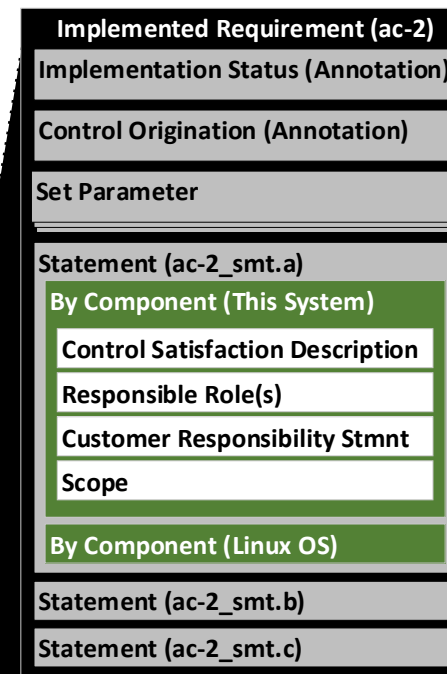
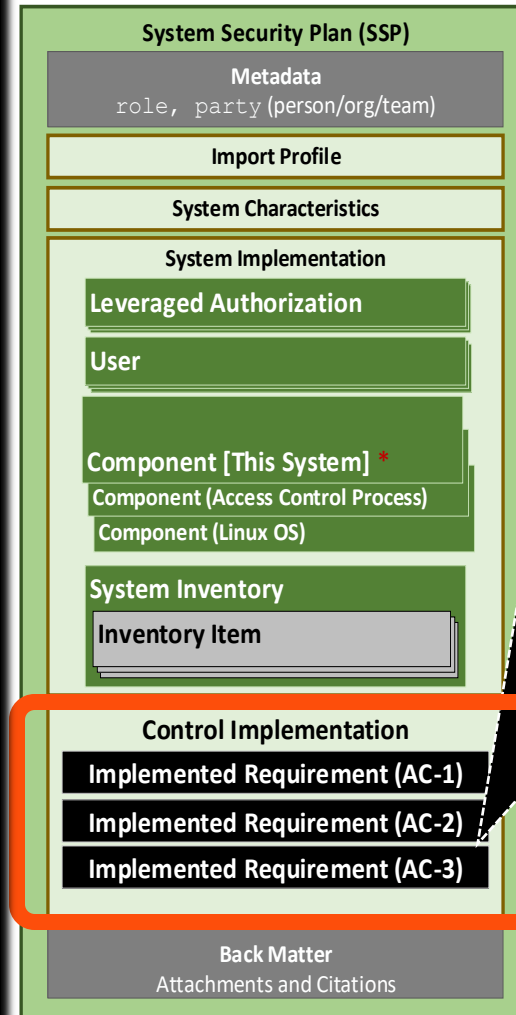
```
▼ system-security-plan [1]: {  
  uuid [1]: uuid,  
  data [1]: { ... },  
  ► import-profile [1]: { ... },  
  ► system-characteristics [1]: { ... },  
  ► system-implementation [1]: { ... },  
  ► control-implementation [1]: { ... },  
  ► back-matter [0 or 1]: { ... }  
}
```



# The SSP Model ...

<https://pages.nist.gov/OSCAL/reference/latest/system-security-plan/json-outline/>

```
▼ system-security-plan [1]: {  
  uuid [1]: uuid,  
  ▶ metadata [1]: { ... },  
  ▶ import-profile [1]: { ... },  
  ▶ system-characteristics [1]: { ... },  
  ▼ control-implementation [1]: {  
    description [1]: markup-multiline,  
    ▶ set-parameters [0 or 1]: { ... },  
    ▼ implemented-requirements [1]: [  
      An array of implemented-requirement objects [1 to ∞]  
      uuid [1]: uuid,  
      control-id [1]: token,  
      ▶ props [0 or 1]: [ ... ],  
      ▶ links [0 or 1]: [ ... ],  
      ▶ set-parameters [0 or 1]: [ ... ],  
      ▶ responsible-roles [0 or 1]: [ ... ],  
      ▶ statements [0 or 1]: [ ... ],  
      ▼ by-components [0 or 1]: [  
        An array of by-component objects [1 to ∞] {  
          component-uuid [1]: uuid,  
          uuid [1]: uuid,  
          description [1]: markup-multiline,  
          ▶ props [0 or 1]: [ ... ],  
          ▶ links [0 or 1]: [ ... ],  
          ▶ set-parameters [0 or 1]: [ ... ],  
          ▶ implementation-status [0 or 1]: { ... },  
          ▶ export [0 or 1]: { ... },  
          ▶ inherited [0 or 1]: [ ... ],  
          ▶ satisfied [0 or 1]: [ ... ],  
          ▶ responsible-roles [0 or 1]: [ ... ],  
          ▶ remarks [0 or 1]: markup-multiline,  
        }  
      ],  
    },  
    ▶ remarks [0 or 1]: markup-multiline,  
  },  
  ▶ back-matter [0 or 1]: { ... }  
}
```





# Even Container Ships Can Sink



'Shifting left' the security by pre-assessing the system's components does not mean the system is secure by default!

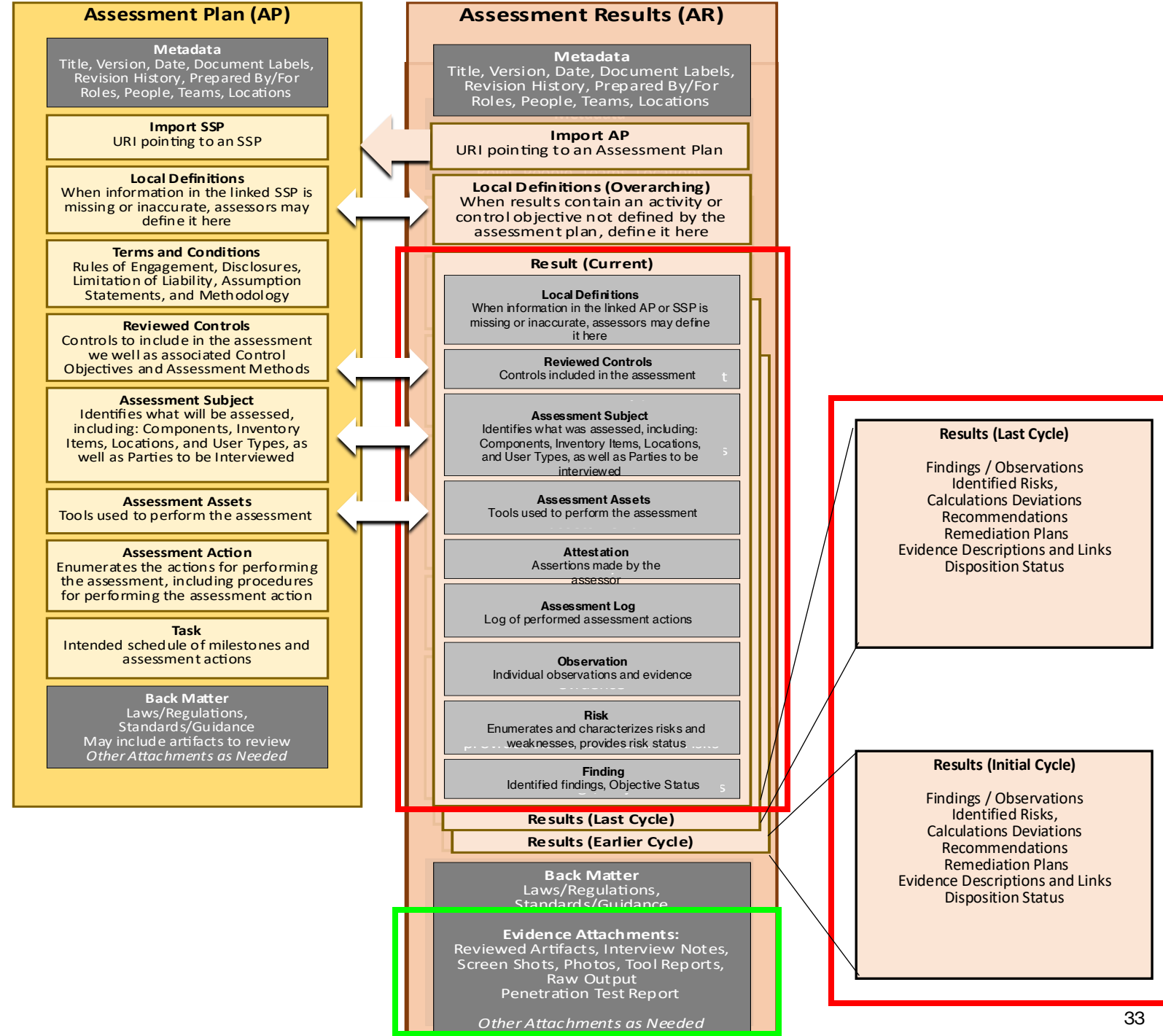
- Review the components in the context of the respective system
- Review the interaction between components
- Get the max return in your investment – be granular with the data and the assessment

# Assessment Plan (AP) & Assessment Results (AR)

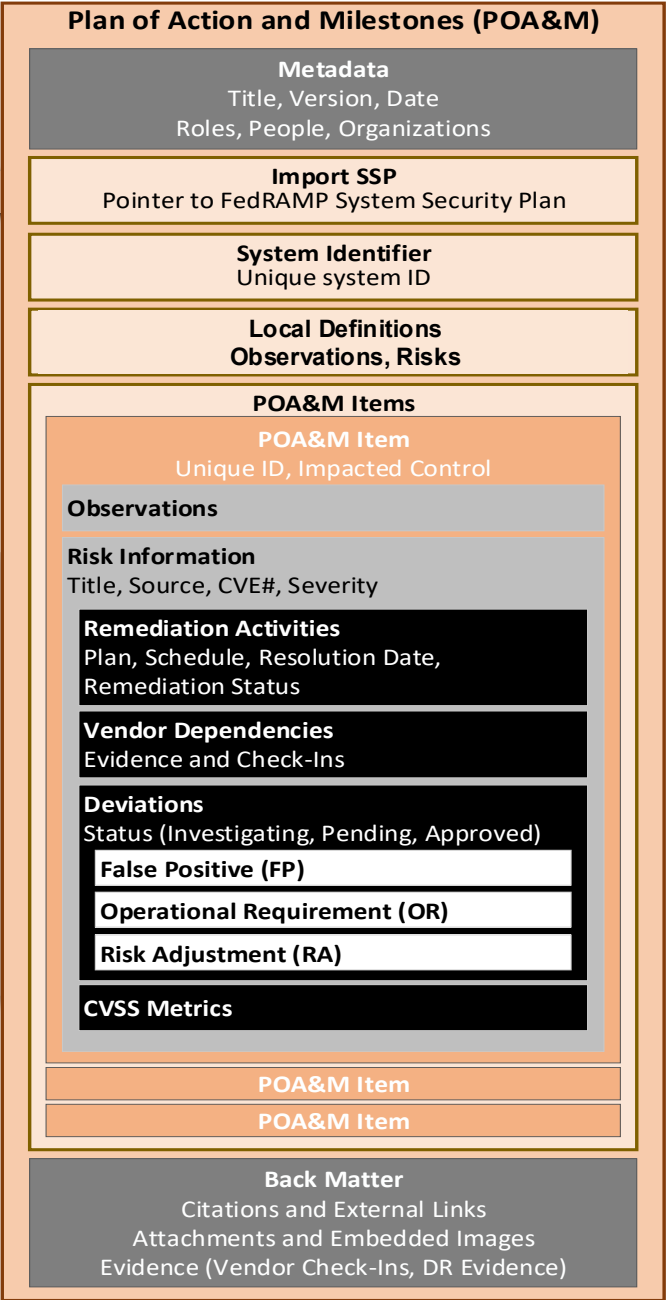
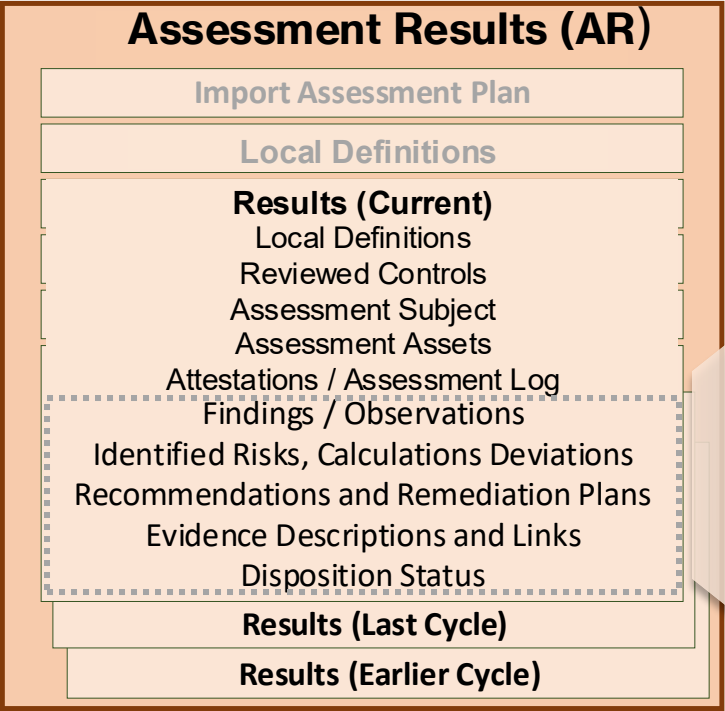
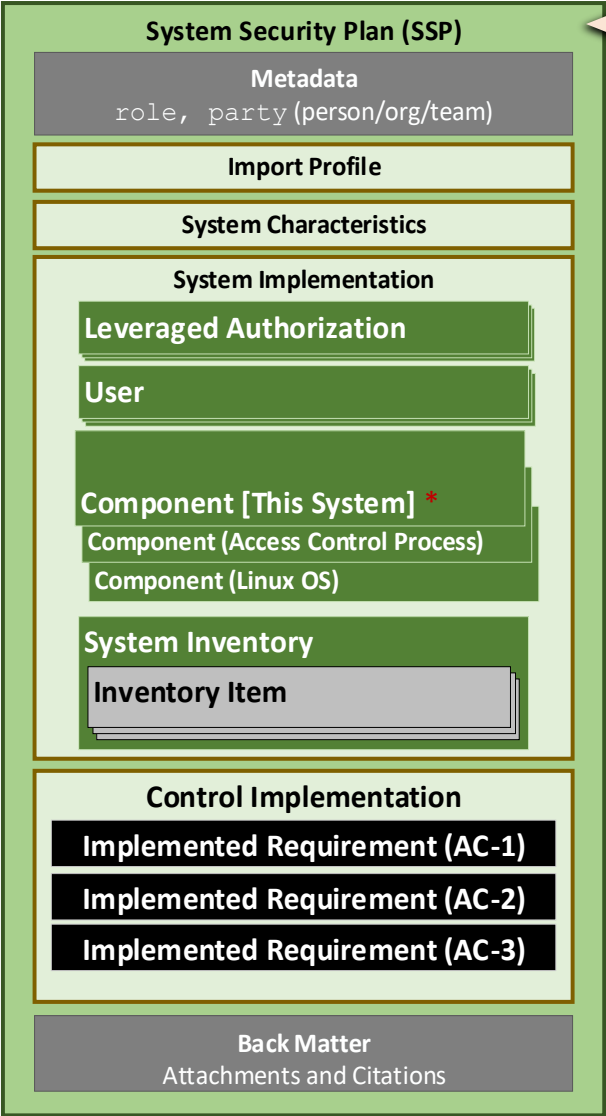
- ❑ Overlapping syntax
- ❑ Similar but distinct purposes
- ❑ **Unique to AR: Results and Evidence**

## Continuous Assessment Approach

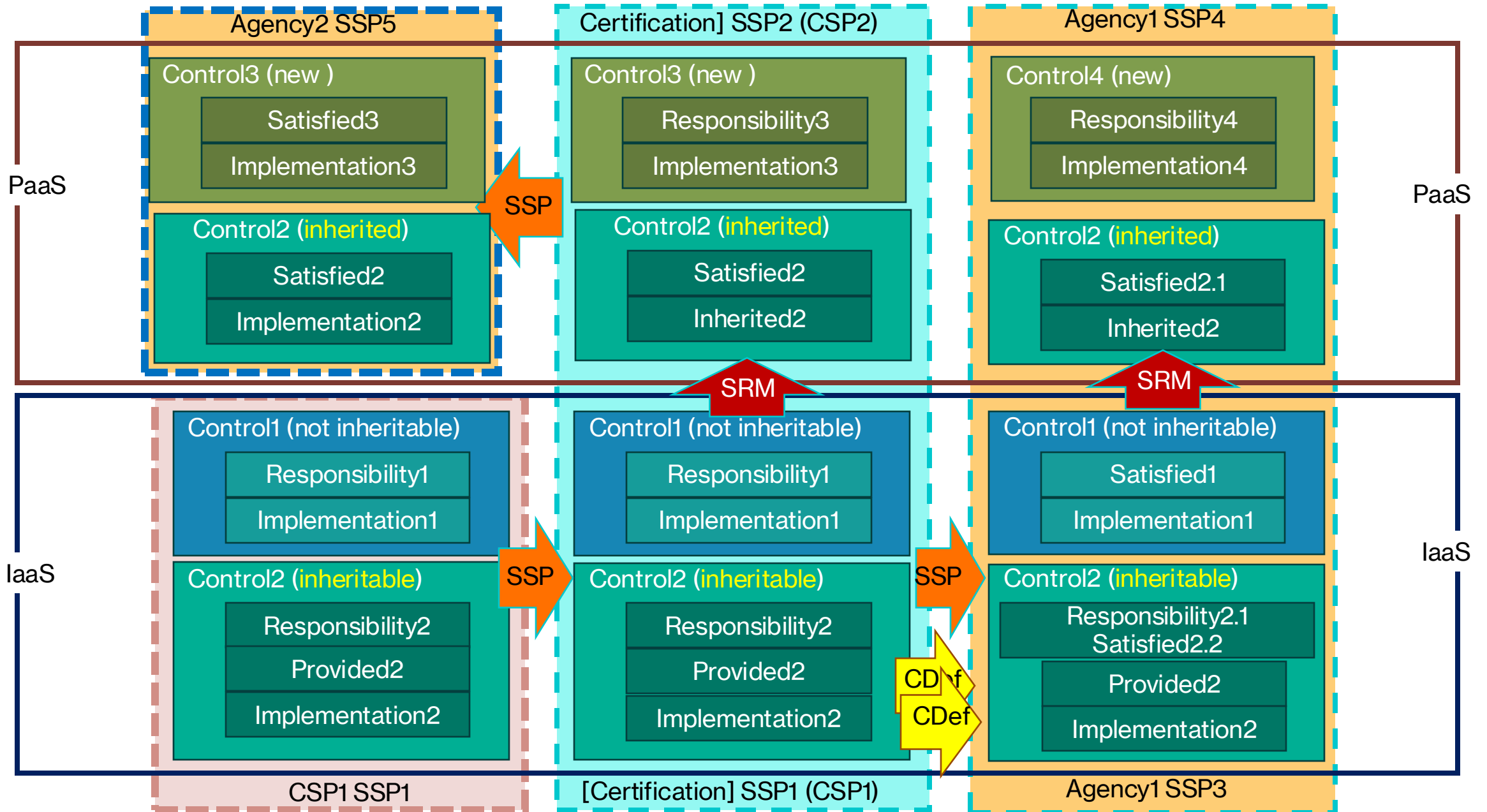
- ❑ **Assessment Plan:**
  - ❑ What should be tested/inspected, how, and with which frequency
- ❑ **Assessment Results:**
  - ❑ Time-slice of results



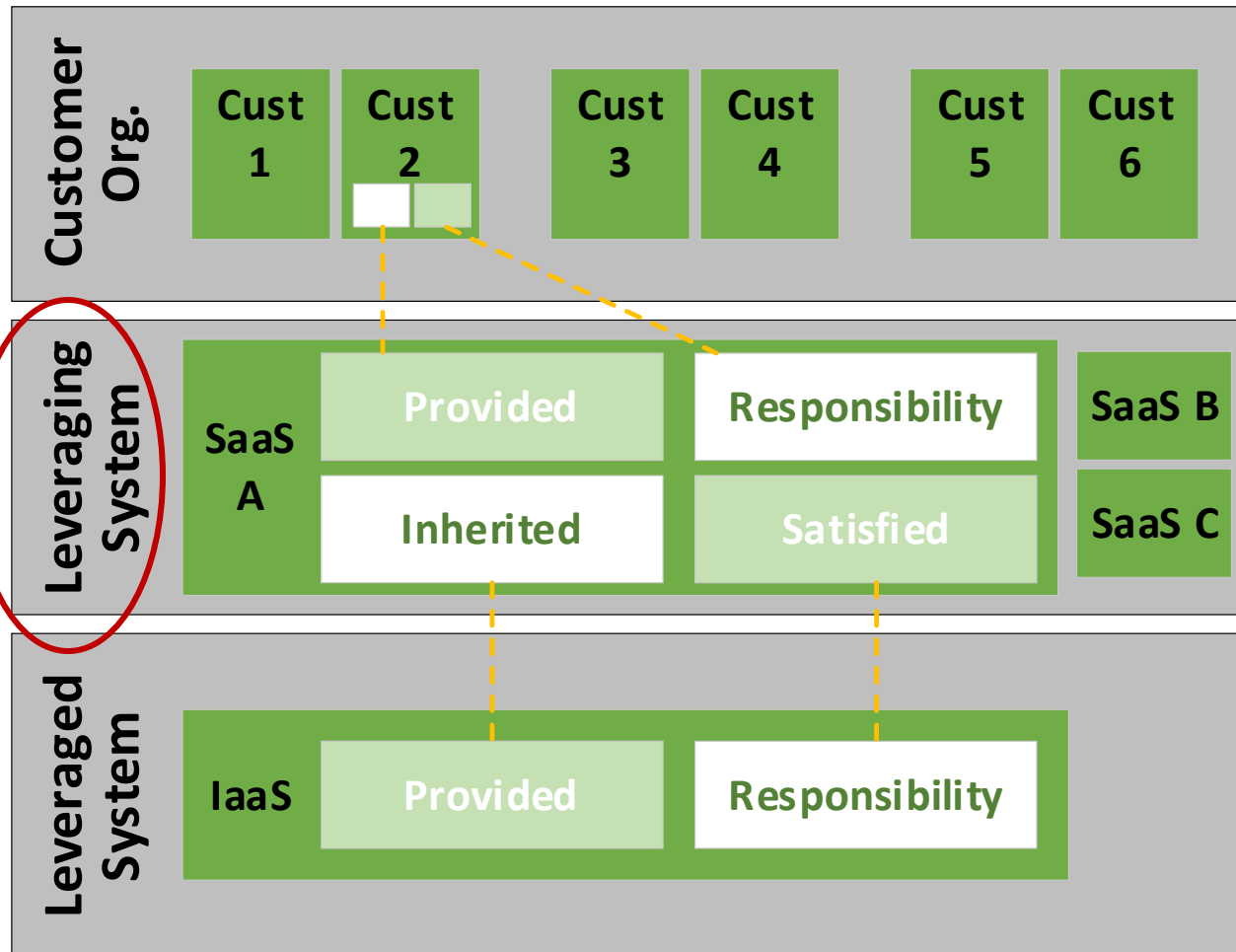
# OSCAL POA&M Model







# The Shared Responsibility (SR) Model



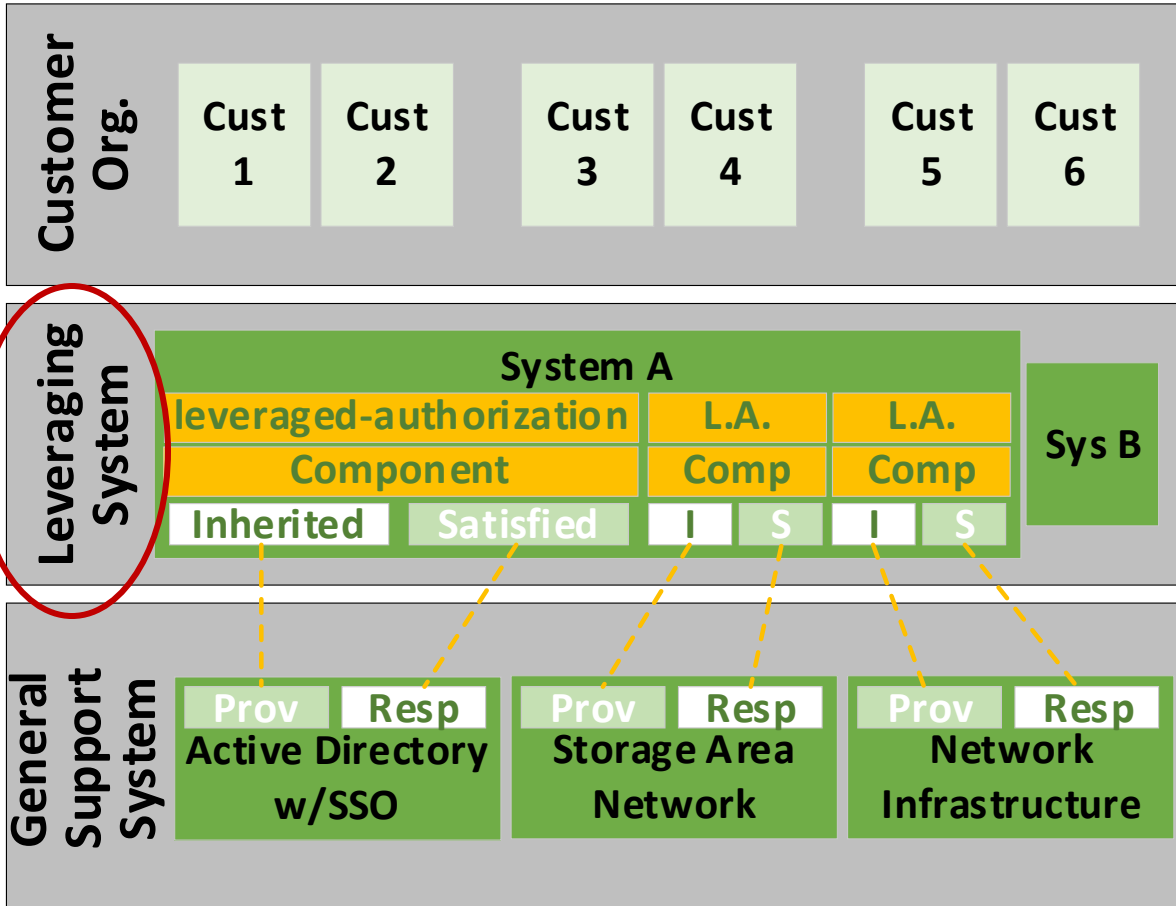
- **Leveraging System:**

- The leveraging system's SSP should:
  - identify what is inherited from a leveraged system
  - identify any addressed responsibilities (as identified by the leveraged system)

In addition to:

- identifying what **may be** inherited by the leveraging system's customers
- any responsibilities the leveraging system's customers must address to fully satisfy a control

# Multi-layer SRMs ...



- **The same syntax is used**
  - It is simply replicated for each leveraged system
- **The Leveraging System's SSP:**
  - Has a separate "leveraged-authorization" assembly for each leveraged system.
  - Has a separate "component" representing each leveraged system.
  - Has a separate "component" representing the leveraged system components associated with inherited capabilities.

# The Prototype Shared Responsibility Model

## - Outline -

```
▶ <provided uuid="uuid" implemented-  
  by="uuid" exportable="boolean"> ...  
</provided> [0 to ∞]  
▶ <responsibility uuid="uuid" provided-  
  uuid="uuid" exportable="boolean"> ...  
</responsibility> [0 to ∞]  
▶ <inherited uuid="uuid" provided-  
  uuid="uuid" implemented-by="uuid"  
  exportable="boolean"> ... </inherited>  
[0 to ∞]  
▶ <satisfied uuid="uuid" responsibility-  
  uuid="uuid" inherited-uuid="uuid"  
  exportable="boolean"> ... </satisfied>  
[0 to ∞]  
▶ <responsible-role role-id="token"> ...  
</responsible-role> [0 to ∞]
```

```
<implemented-requirement uuid="uuid" control-  
id="token"> [1 to ∞]  
  ▶ <prop name="token" uuid="uuid" ns="uri"  
    value="string" class="token" group="token"> ...  
  </prop> [0 to ∞]  
  ▶ <link href="uri-reference" rel="token" media-  
    type="string" resource-fragment="string"> ...  
  </link> [0 to ∞]  
  ▶ <set-parameter param-id="token"> ... </set-  
    parameter> [0 to ∞]  
  ▶ <responsible-role role-id="token"> ...  
  </responsible-role> [0 to ∞]  
  ▶ <statement statement-id="token" uuid="uuid"> ...  
  </statement> [0 to ∞]  
  ▶ <by-component component-uuid="uuid"  
    uuid="uuid"> ... </by-component> [0 to ∞]  
  ▶ <remarks>markup-multiline</remarks> [0 or 1]  
</implemented-requirement>
```

```
▼ <shared-responsibility uuid="uuid"> [1]  
  ▶ <metadata> ... </metadata> [1]  
  ▼ <source-ssp ssp-uuid="uuid"> [0 or 1]  
    ▶ <title>markup-line</title> [0 or 1]  
    ▶ <published>date-time-with-timezone</published> [0  
      or 1]  
    ▶ <last-modified>date-time-with-timezone</last-  
      modified> [0 or 1]  
    ▶ <version>string</version> [0 or 1]  
    ▶ <date-authorized>date</date-authorized> [0 or 1]  
    ▶ <party-uuid>uuid</party-uuid> [1]  
    ▶ <referenced-profile href="uri-reference"/> [0 or 1]  
    ▶ <prop name="token" uuid="uuid" ns="uri"  
      value="string" class="token" group="token"> ...  
    </prop> [0 to ∞]  
    ▶ <link href="uri-reference" rel="token" media-  
      type="string" resource-fragment="string"> ... </link>  
    [0 to ∞]  
    ▶ <remarks>markup-multiline</remarks> [0 or 1]  
  </source-ssp>  
  ▼ <control-implementation> [1]  
    ▶ <description>markup-multiline</description> [1]  
    ▶ <set-parameter param-id="token"> ... </set-parameter>  
    [0 to ∞]  
    ▶ <implemented-requirement uuid="uuid" control-  
      id="token"> ... </implemented-requirement> [1 to ∞]  
  </control-implementation>  
  ▶ <back-matter> ... </back-matter> [0 or 1]  
</shared-responsibility>
```

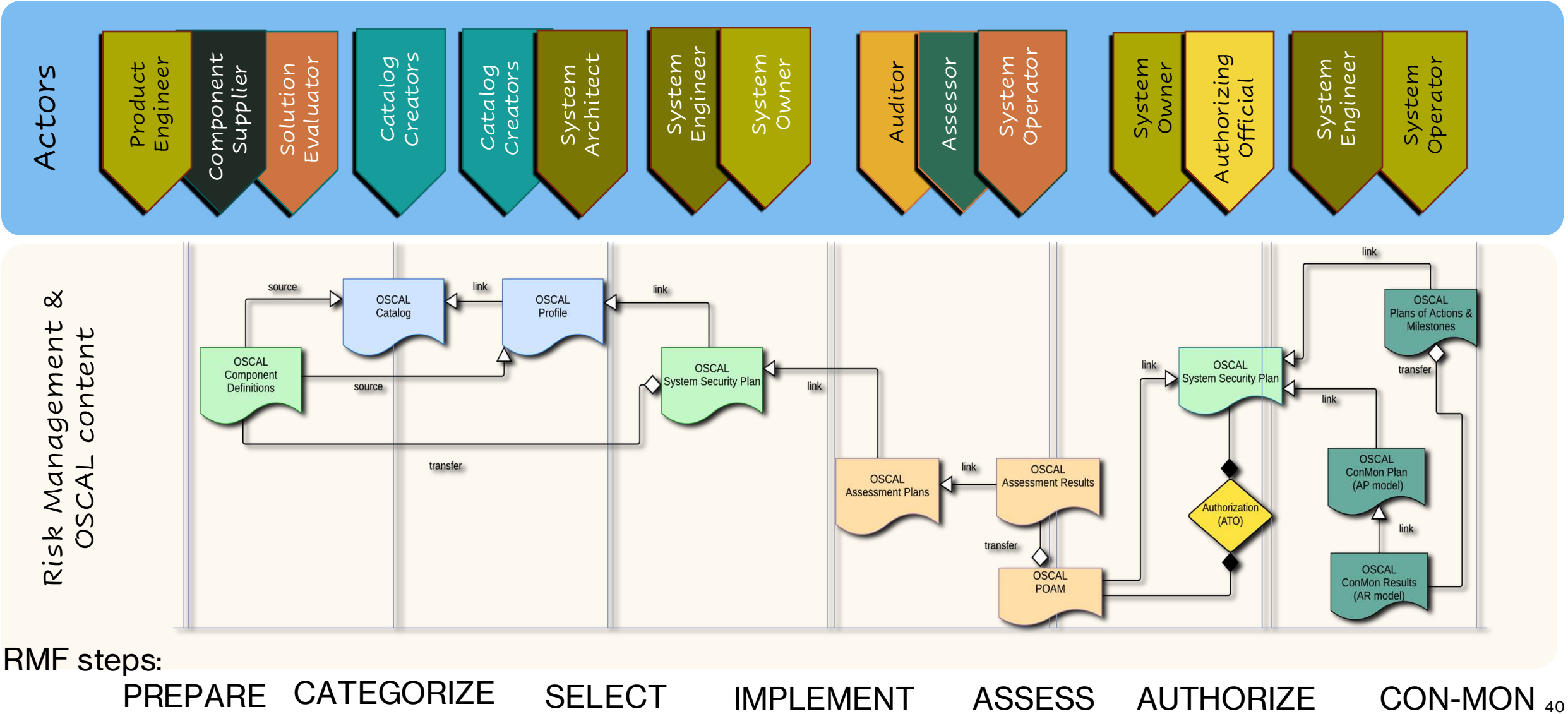


# The Prototype Control Mapping Model

## - Outline -

```
▼ <mapping-collection uuid="uuid"> [1]
  ▶ <metadata> ... </metadata> [1]
  ▶ <provenance method="string" matching-rationale="string" status="string">
    ... </provenance> [1]
  ▼ <mapping uuid="uuid"> [1 to ∞]
    ▶ <source-resource type="token" href="uri-reference"> ... </source-
      resource> [1]
    ▶ <target-resource type="token" href="uri-reference"> ... </target-
      resource> [1]
    ▼ <map uuid="uuid" ns="uri" matching-rationale="string"> [1 to ∞]
      ▶ <relationship>token</relationship> [1]
      ▶ <source type="token" id-ref="string"> ... </source> [1 to ∞]
      ▶ <target type="token" id-ref="string"> ... </target> [1 to ∞]
      ▶ <qualifier subject="string" predicate="string"
        category="string"> ... </qualifier> [0 to ∞]
      ▶ <prop name="token" uuid="uuid" ns="uri" value="string"
        class="token" group="token"> ... </prop> [0 to ∞]
      ▶ <link href="uri-reference" rel="token" media-type="string"
        resource-fragment="string"> ... </link> [0 to ∞]
      ▶ <remarks>markup-multiline</remarks> [0 or 1]
    </map>
  </mapping>
  ▶ <source-gap-summary uuid="uuid"> ... </source-gap-summary> [0 or 1]
  ▶ <target-gap-summary uuid="uuid"> ... </target-gap-summary> [0 or 1]
  ▶ <back-matter> ... </back-matter> [0 or 1]
</mapping-collection>
```

# OSCAL Models & RMF





# OSCAL Adopters Around the Globe







# The future of OSCAL ...



```
operation == "MIRROR_X":  
    mirror_mod.use_x = True  
    mirror_mod.use_y = False  
    mirror_mod.use_z = False  
    operation == "MIRROR_Y":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = True  
    mirror_mod.use_z = False  
    operation == "MIRROR_Z":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = False  
    mirror_mod.use_z = True
```

```
@selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob.name))  
mirror_ob.select = 0  
bpy.context.selected_objects  
data.objects[one.name].select  
print("please select exactly one object")
```

```
--- OPERATOR CLASSES ---
```

```
types.Operator):  
    X mirror to the selected  
    object.mirror_mirror_x"  
    mirror X"
```



The **OSCAL** project is developed openly on GitHub.com



**Repository:**

<https://github.com/usnistgov/OSCAL>



**Project Website:**

<https://www.nist.gov/oscal>



Contact the team: [oscal@nist.gov](mailto:oscal@nist.gov)

# THANK YOU !!