Actions Beyond Words:

Automating Audits for Streamlined Cybersecurity Compliance in Europe

Continuous Proactive Security with OSCAL

Going Beyond 'Shifting Left Security'

Dr. Michaela Iorga

Director, OSCAL Program

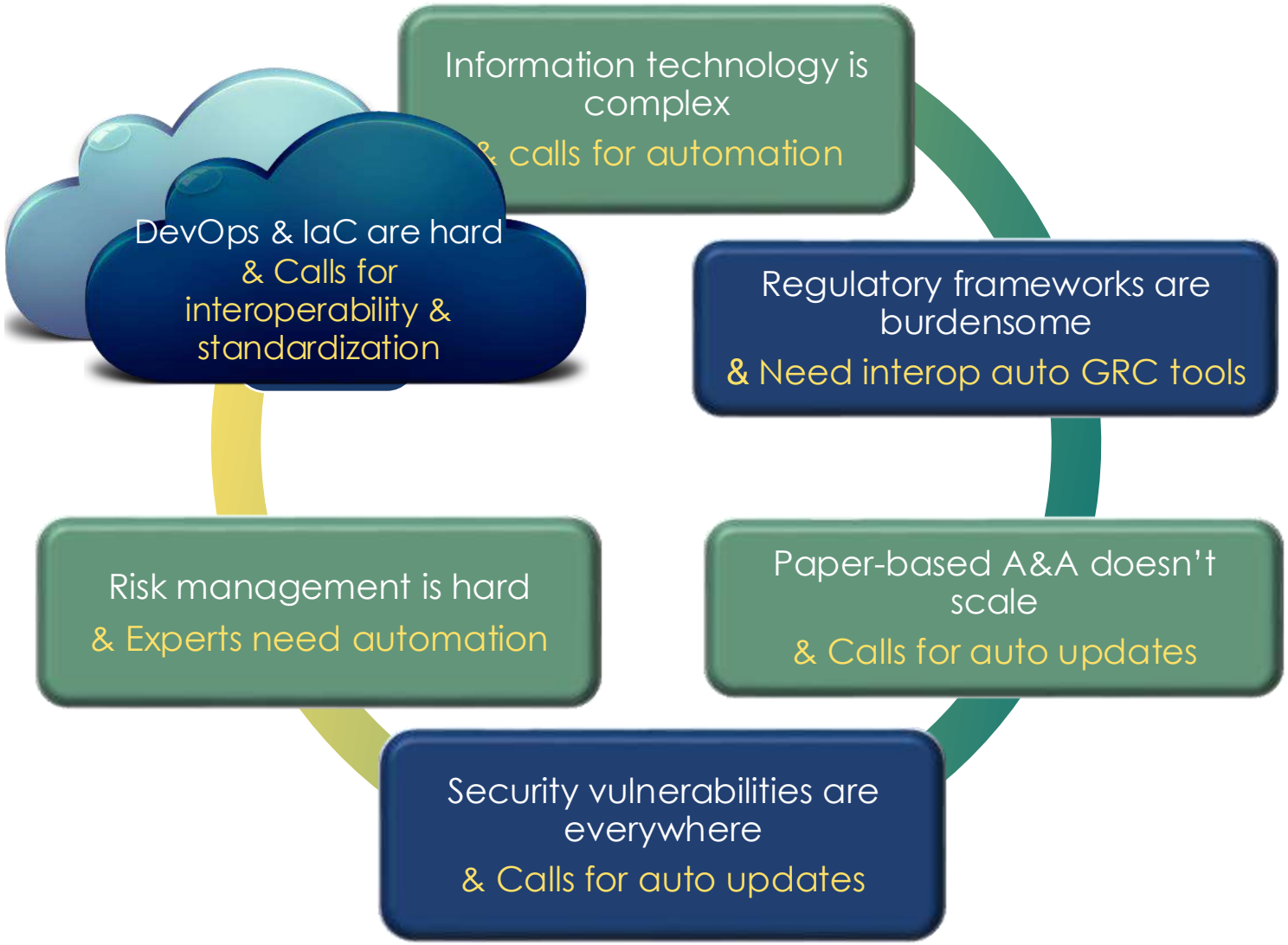
ITL/NIST

Agenda

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

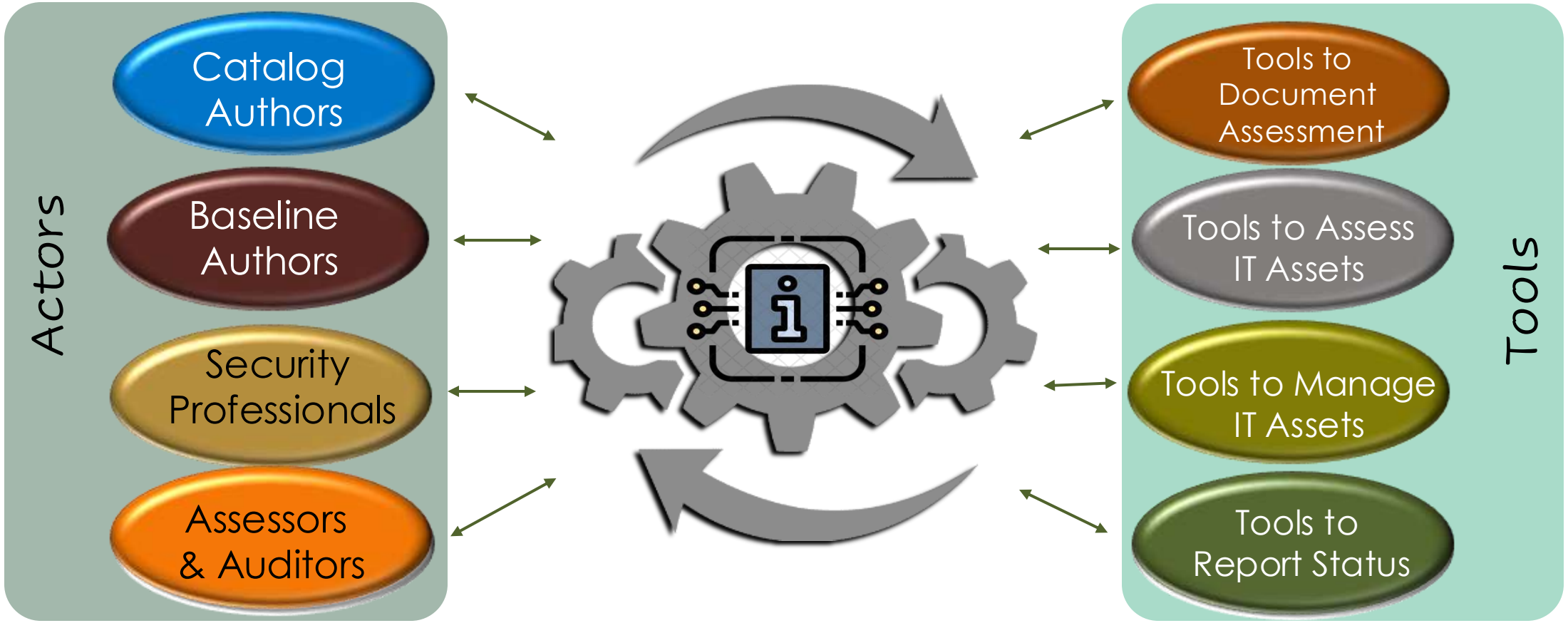
The Problem …


Before the audit
During the audit
After the audit


Information technology is complex
& calls for automation
Regulatory frameworks are burdensome
& Need interop auto GRC tools
Paper-based A&A doesn't scale
& Calls for auto updates
Security vulnerabilities are everywhere
& Calls for auto updates
Risk management is hard
& Experts need automation
DevOps & IaC are hard
& Calls for interoperability & standardization

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.

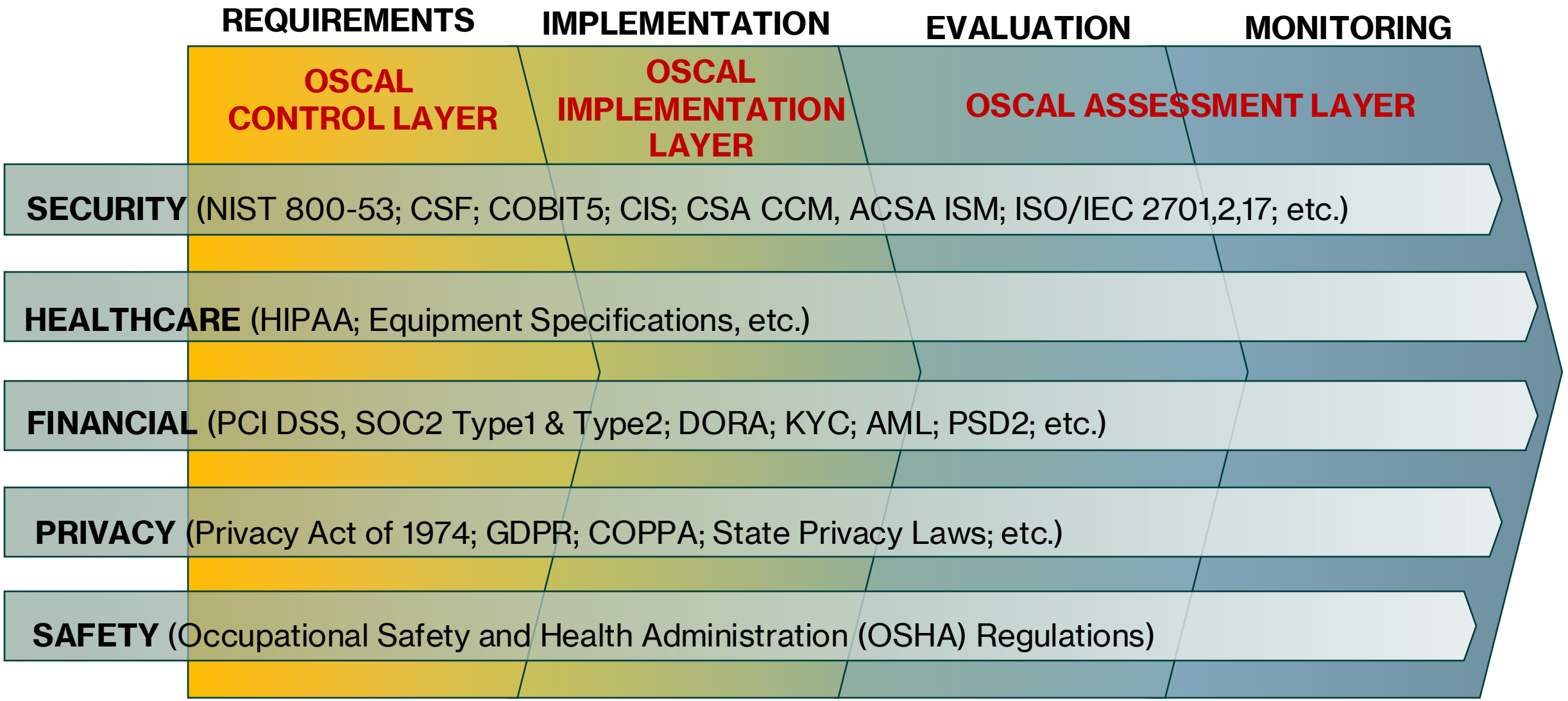
Design Goals ...

- ❑ 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

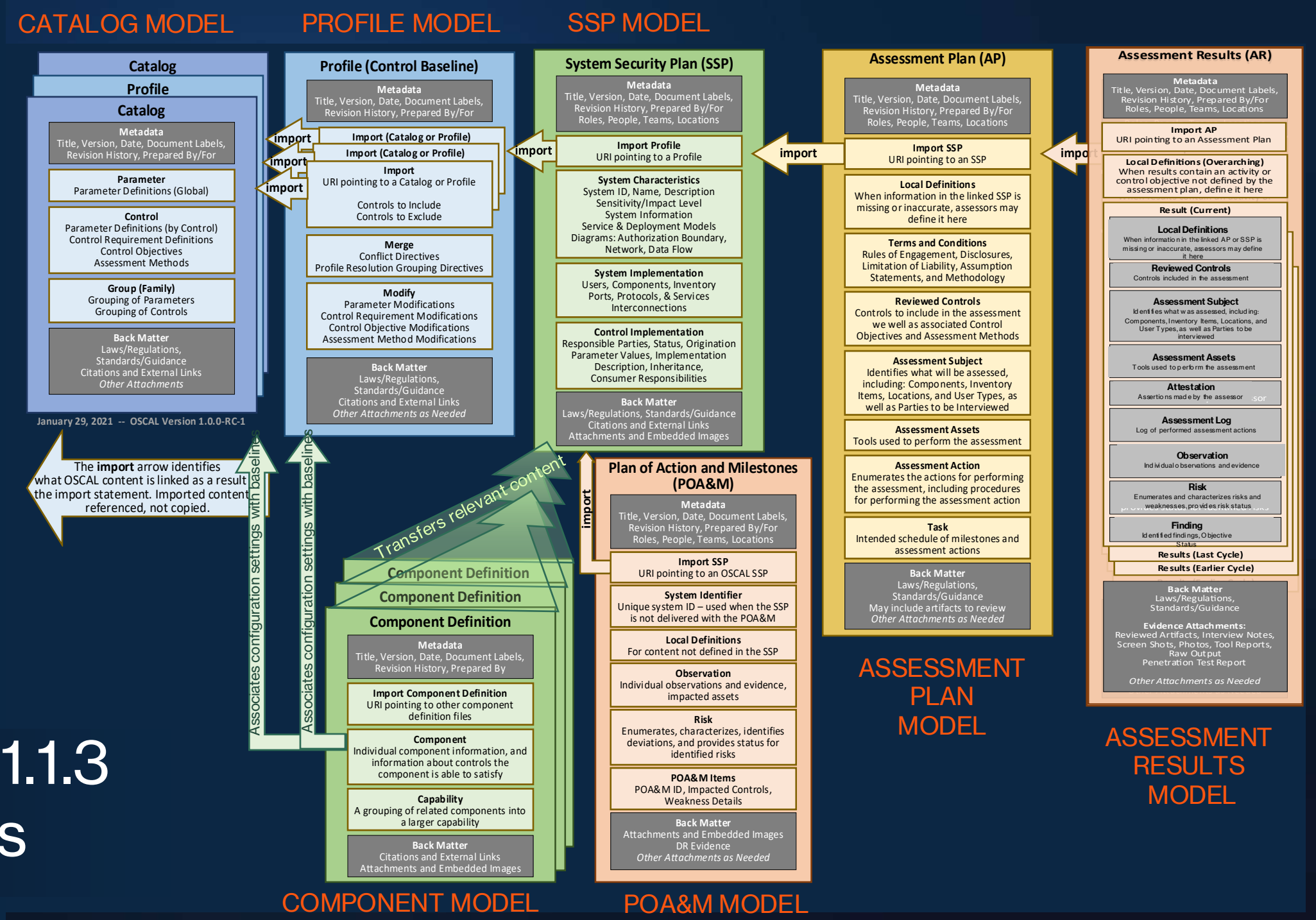
- ❑ Open
- ❑ Security
- ❑ Controls
- ❑ Assessment
- ❑ Language

- ❑ Free for everyone
- ❑ Compliance (security, privacy, safety, etc...)
- ❑ Requirements that needs assessment
- ❑ Evaluation of the safeguard implemented in response of a set of requirements
- ❑ Digital representation – a translation of the information for machines to consume.

Applicable to Any Domain ...



OSCAL v1.1.3 Models



https://nist.gov/oscal

NIST

OSCAL: the Open Security Controls Assessment Language

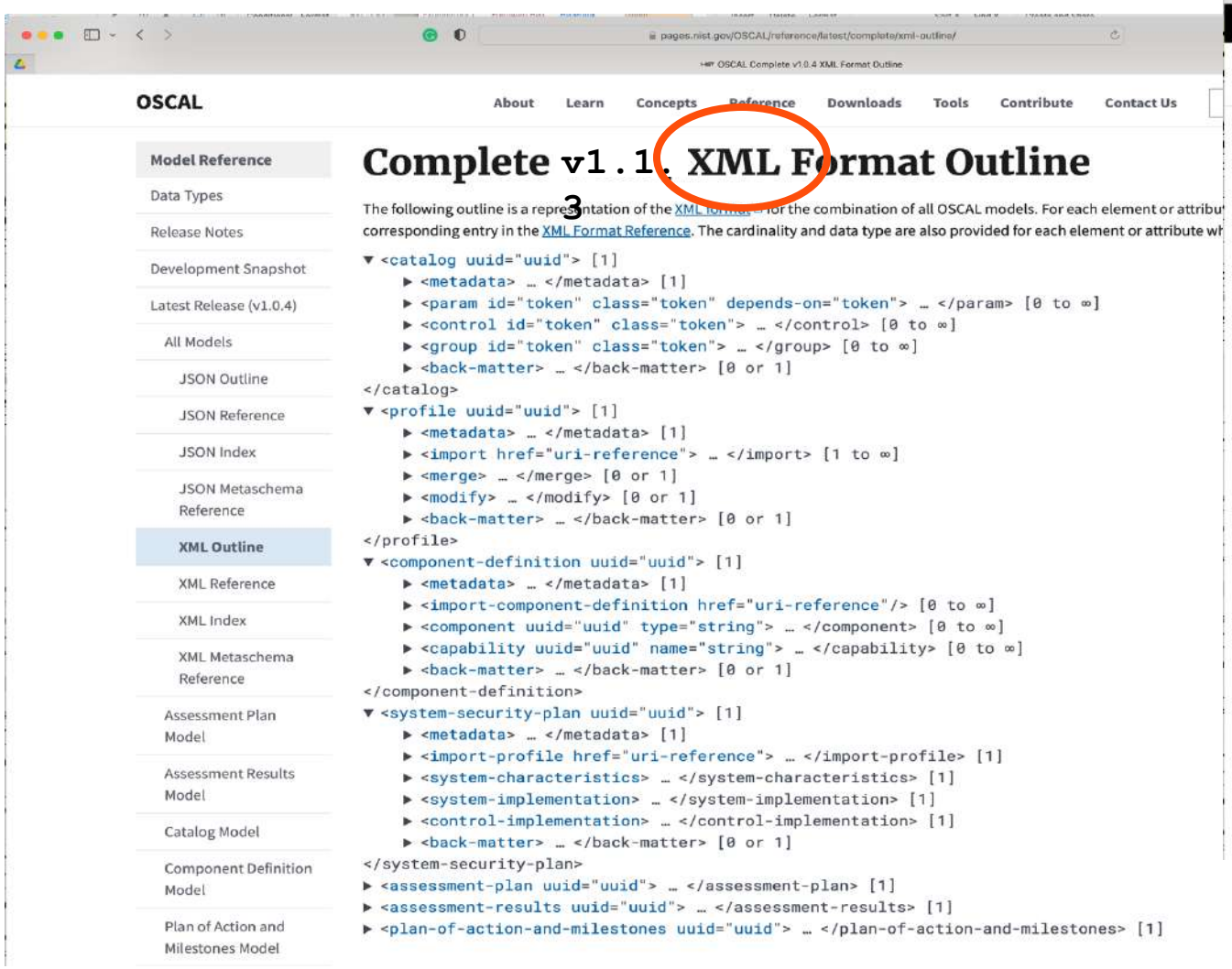
Get involved | Contact Us | Github

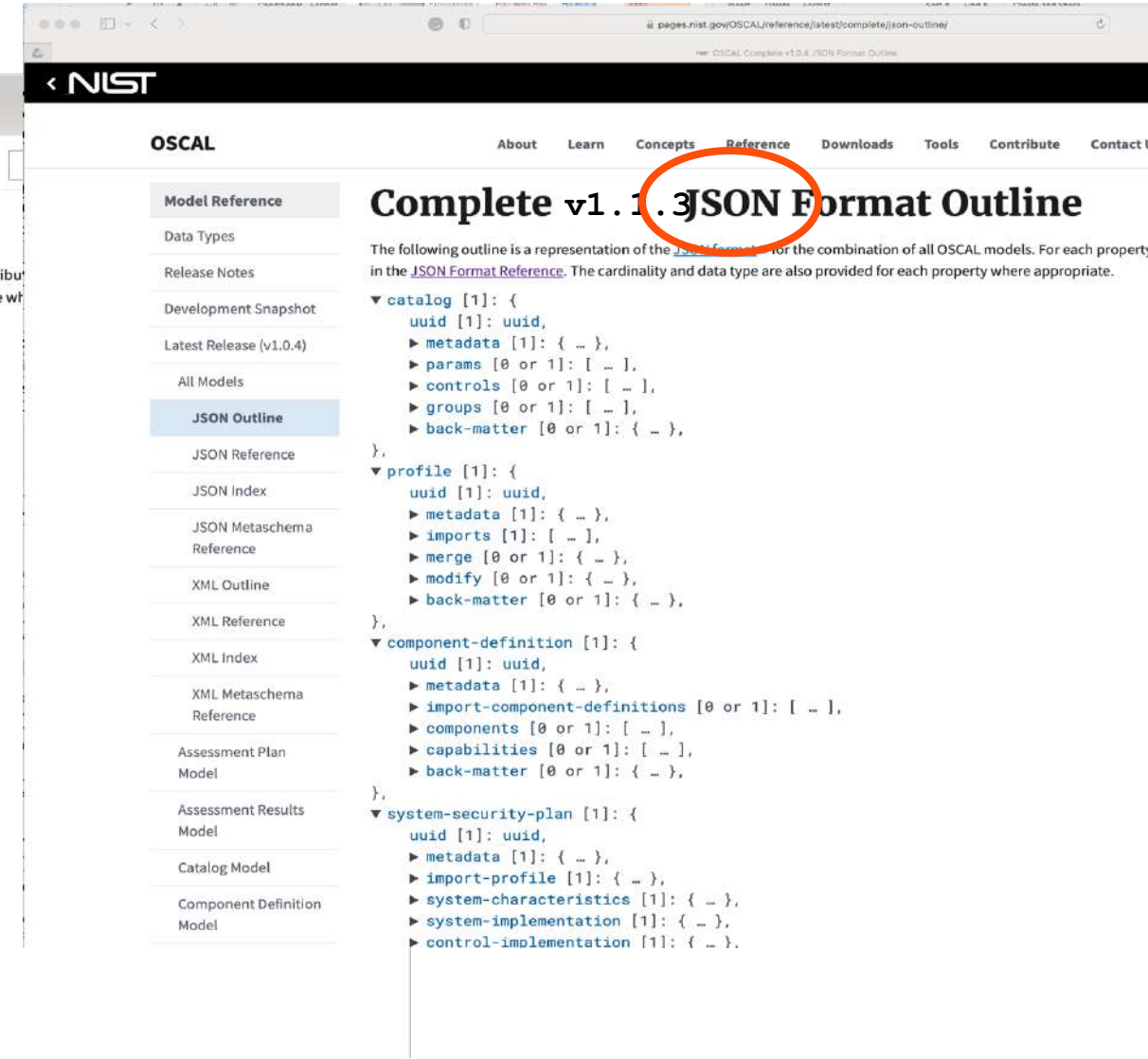
About | Learn | Concepts | Reference | Downloads | Tools | Contribute | Contact Us

Providing control-related information in machine-readable formats.

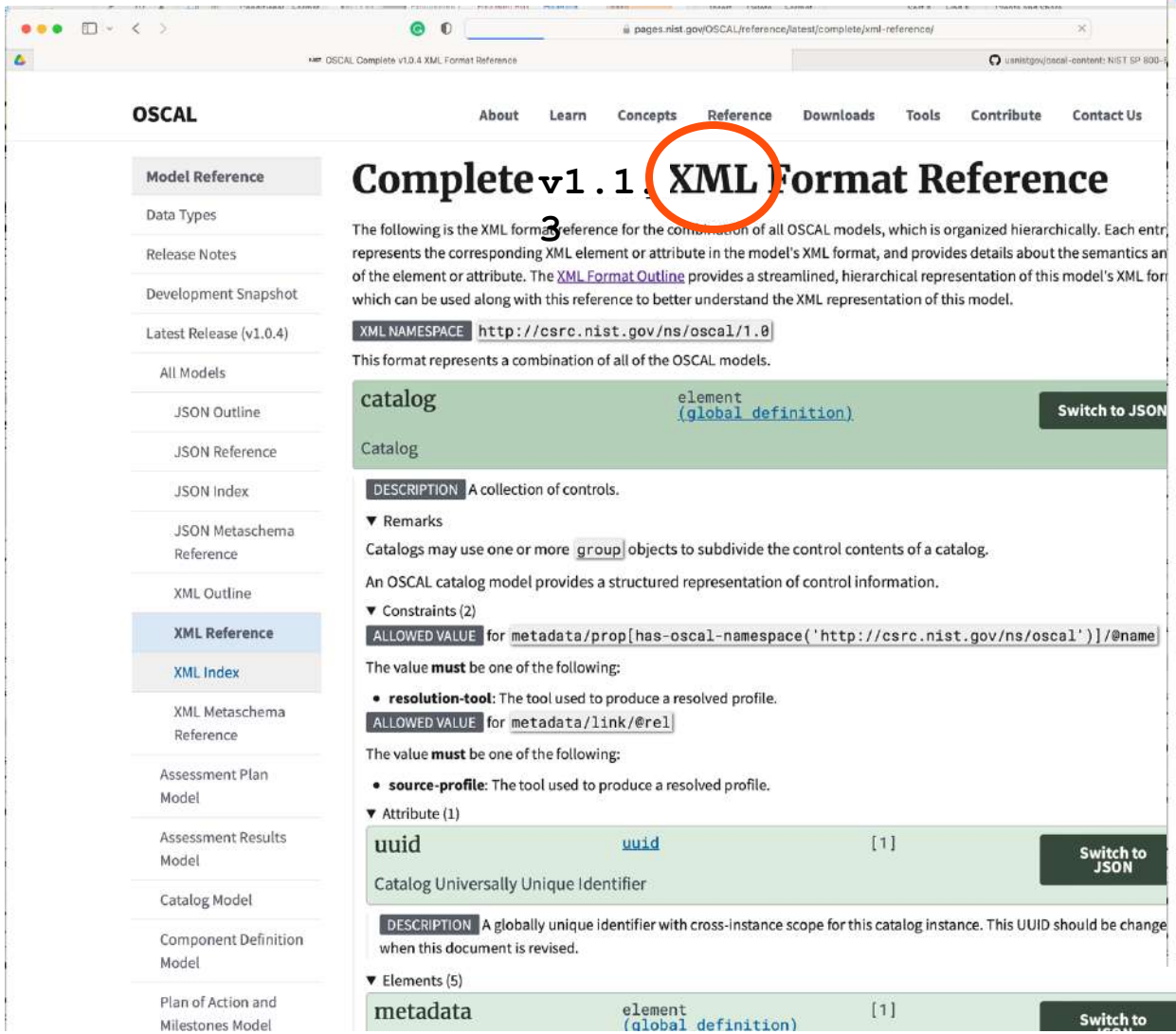
NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.

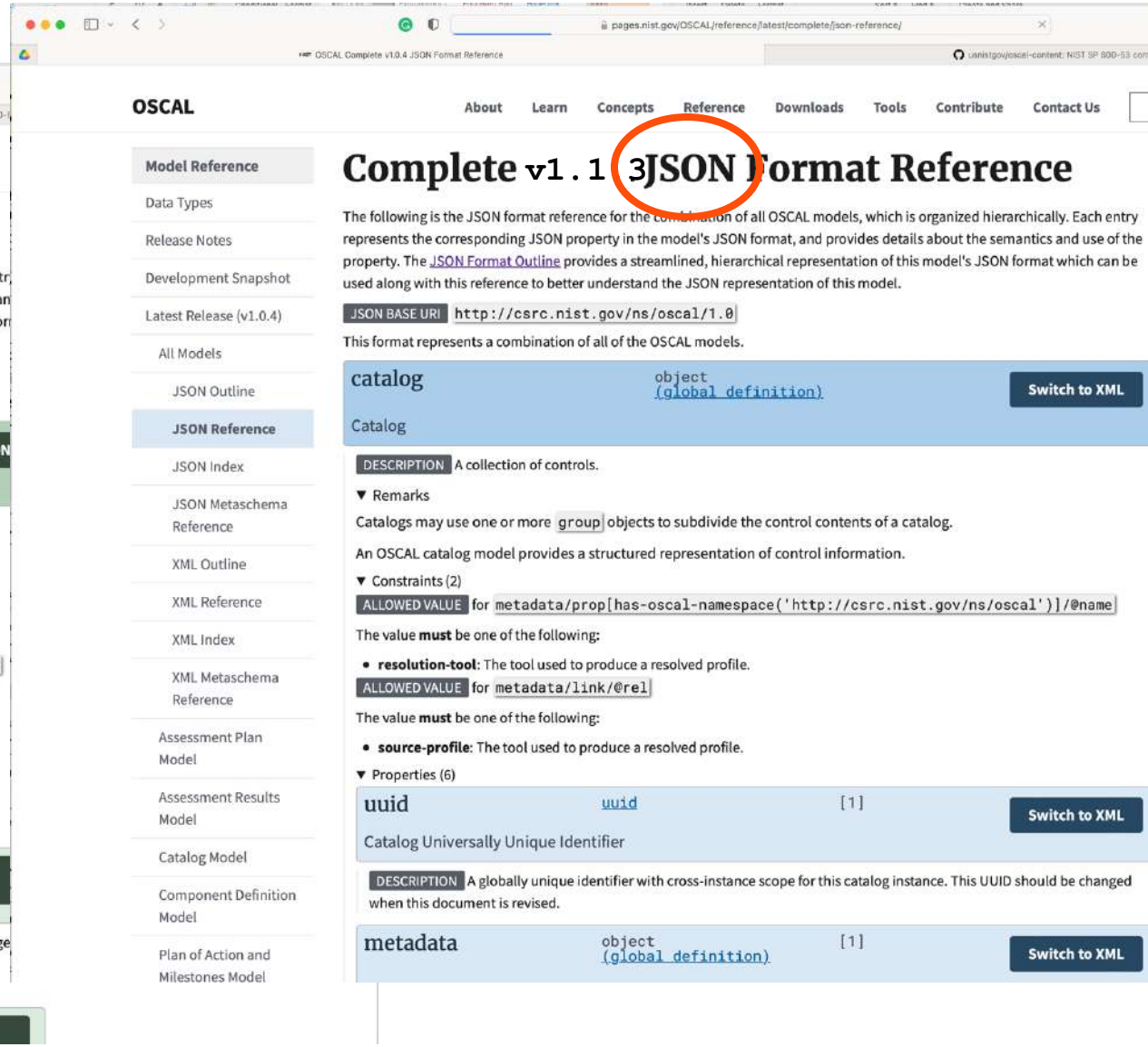
OSCAL Models' Outline





OSCAL Models' References





OSCAL Releases ...

FIRST OSCAL 1.0.0

RELEASED ON JUNE 7, 2021

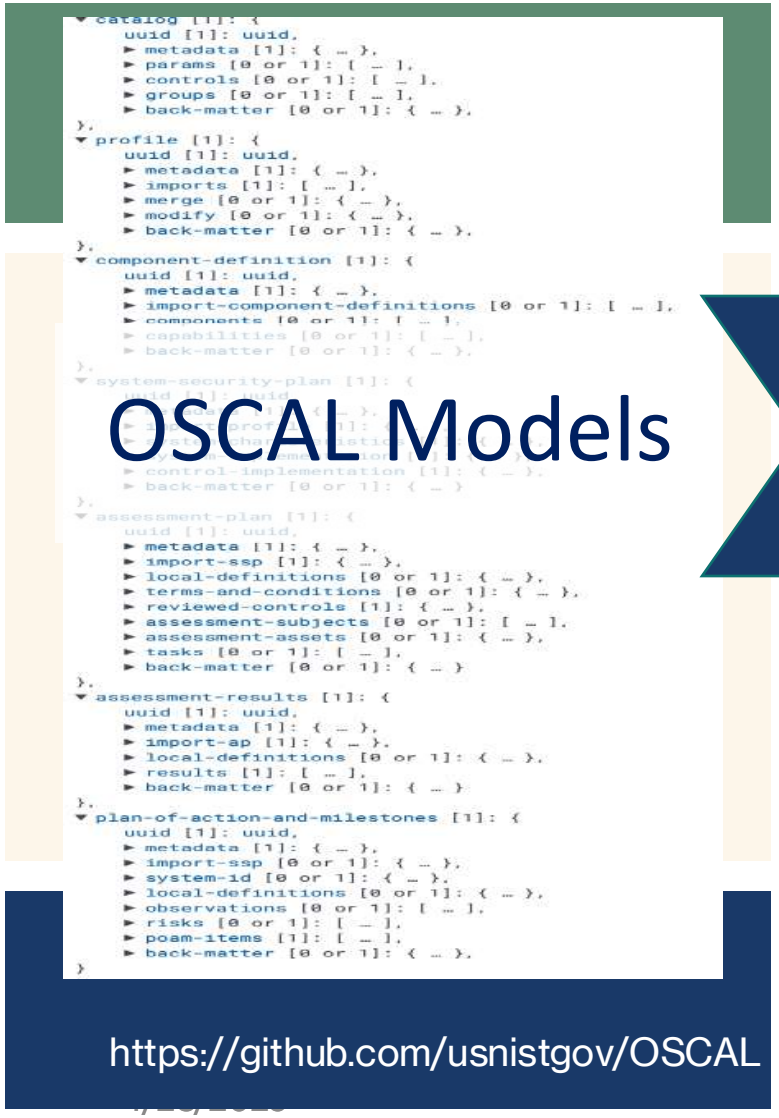
LATEST: OSCAL 1.1.3

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

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

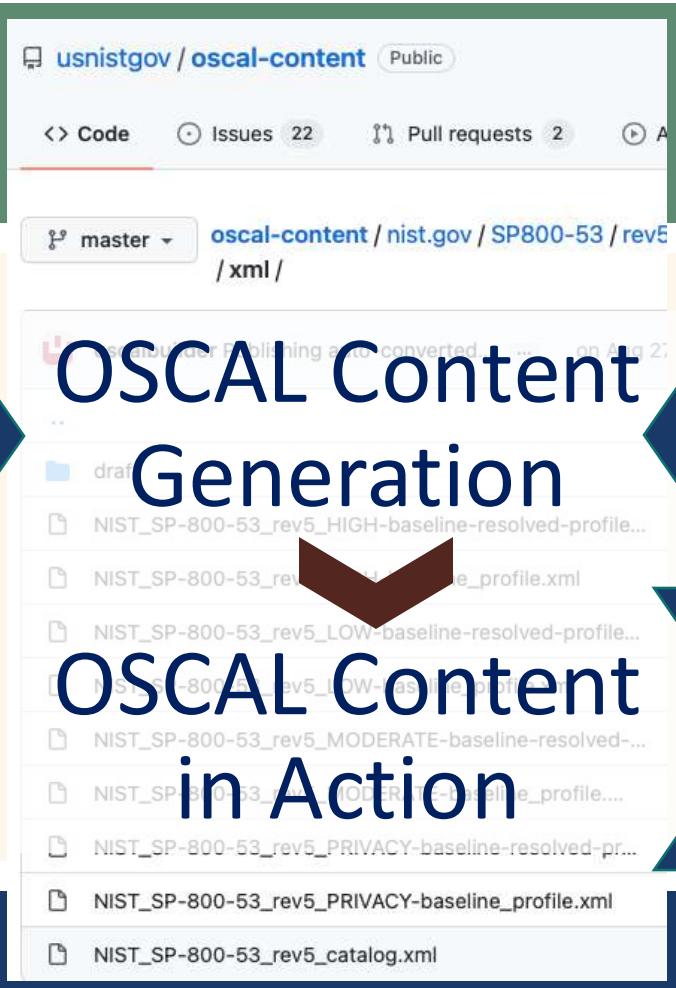
Latest OSCAL patch release : 1.1.3 - backwards compatible.

OSCAL Ecosystem



OSCAL Models

https://github.com/usnistgov/OSCAL



OSCAL Content Generation

OSCAL Content in Action

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

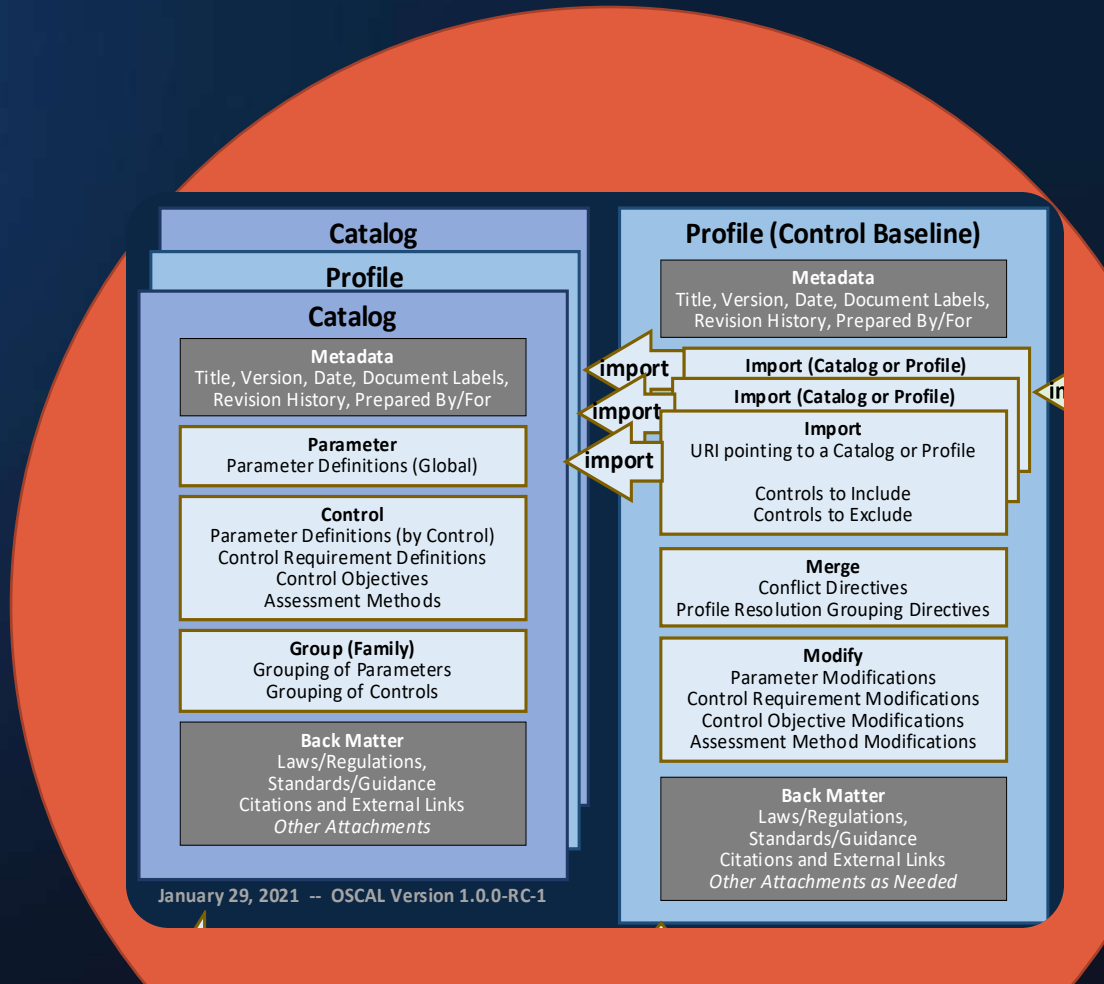
Name	Provider/Developer	Description	Type
Compliance trestle	IBM	A python SDK and command line tool which manipulates OSCAL structures and supports transformation of data into OSCAL.	open source
OSCAL Java Library	NIST OSCAL Project	A Java-based programming API for reading and writing content conformant 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	A variety of Extensible Stylesheet Language Transformations (XSLT) and Cascading Style Sheets (CSS), and related utilities for authoring, converting, and publishing OSCAL content in various forms.	open source
XML Jelly Sandwich	Wendell Piez (NIST)	Interactive XSLT in the browser includes OSCAL demonstrations.	open source
Xacta 360		Xacta 360 is a cyber risk management and [illegible] platform that supports system security plans (SSPs) in OSCAL format. Future OSCAL capabilities are forthcoming as the [illegible]	license
Atlasity: Continuous Compliance Automation	C2 Labs	[illegible] 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 blog post: Atlasity Delivers Free Tools to Create OSCAL Content.	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

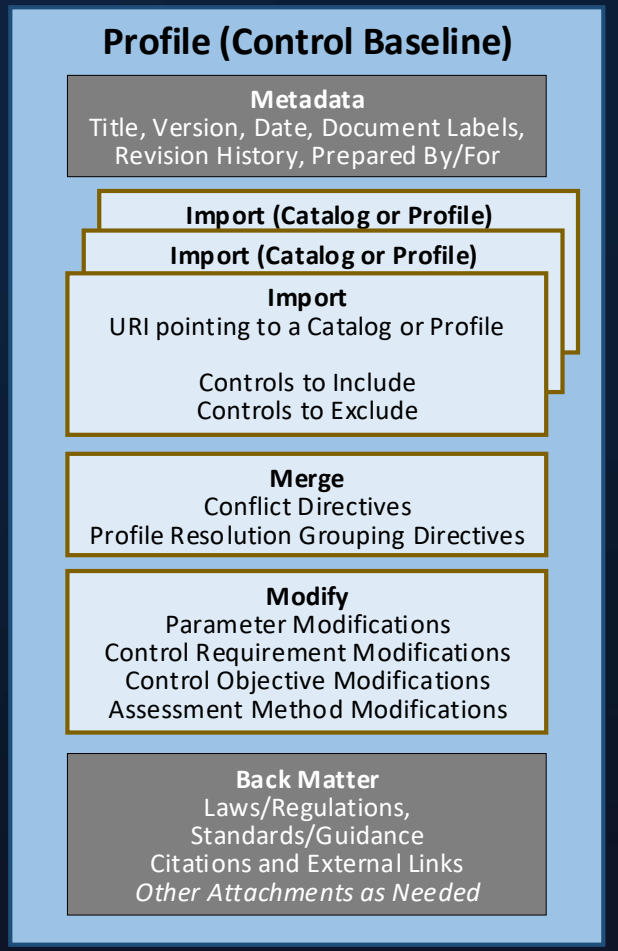
Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links
Other Attachments

```
▼ <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>
```

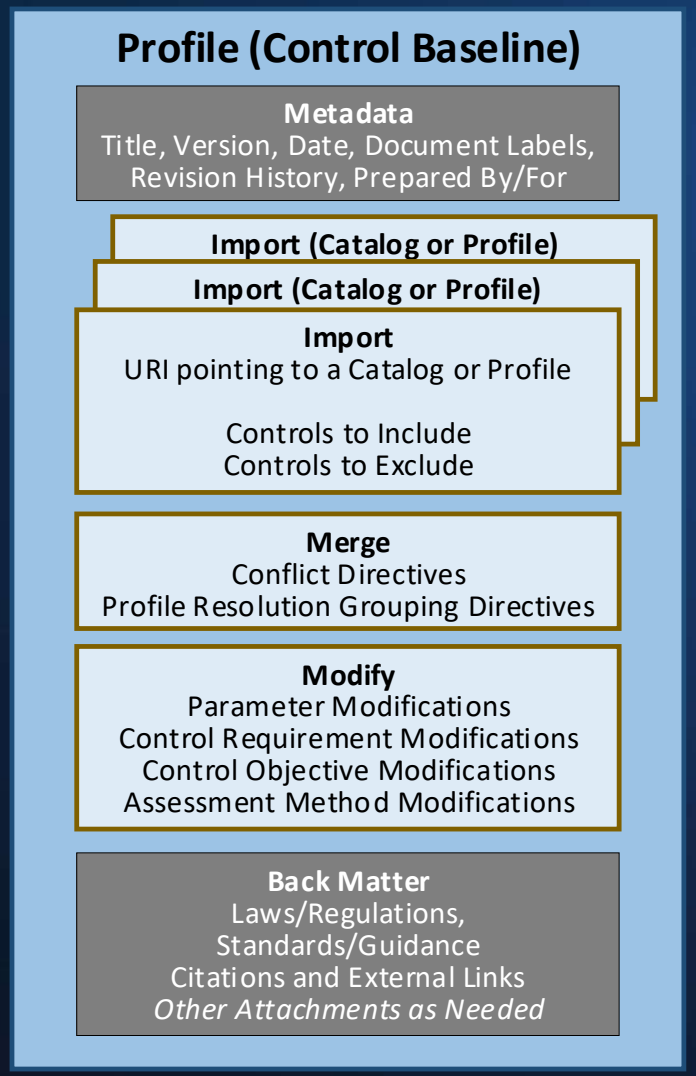
OSCAL Profile Model

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



OSCAL Profile Model



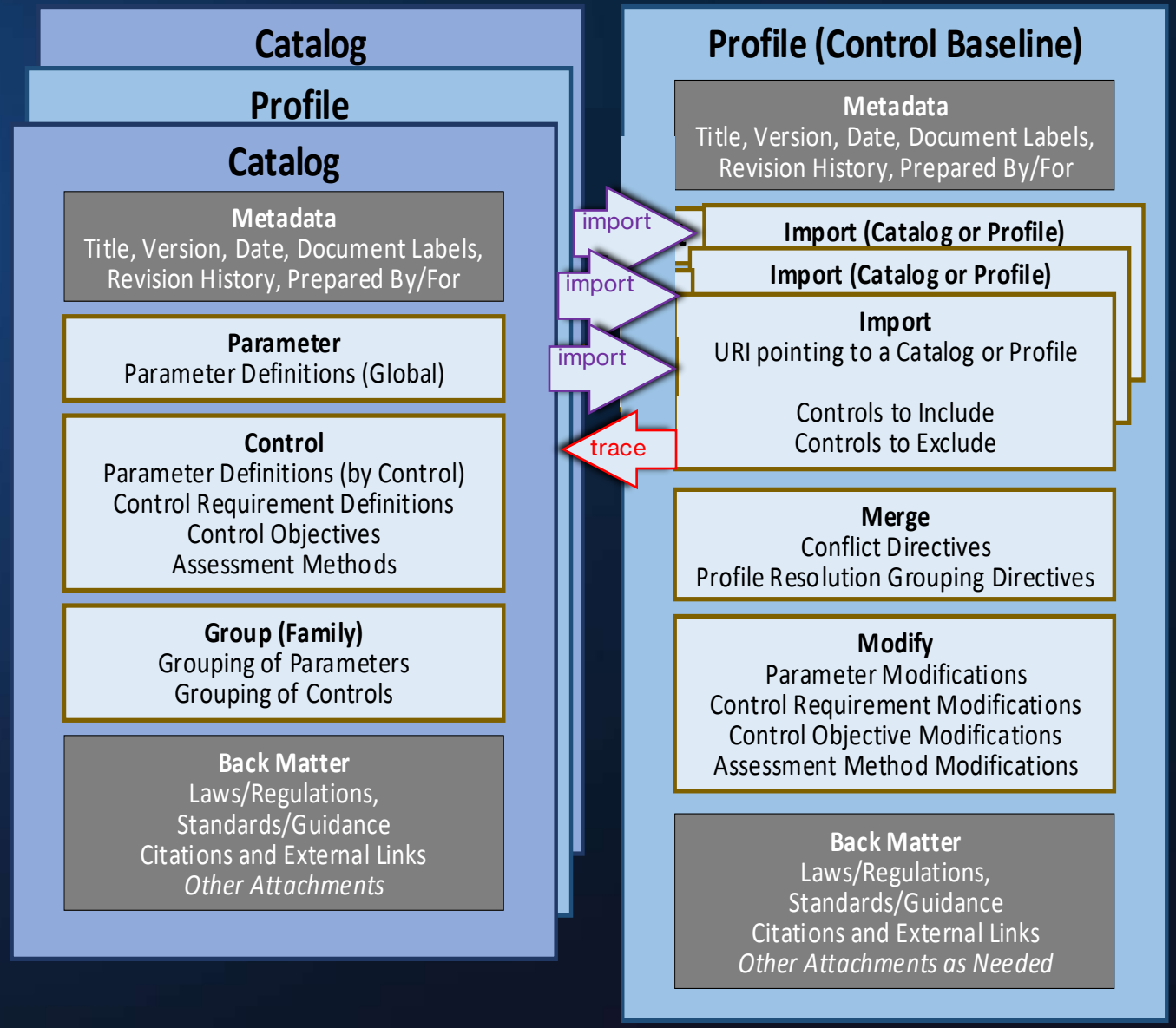

```
▼<profile uuid="uuid"> [1]
  ▶<metadata> … </metadata> [1]
  ▼<import href="uri-reference"> [1 to ∞]
      A choice of:
        ▶<include-all/> [1]
        ▶<include-controls with-child-controls="token"> … </include-controls> [1 to ∞]
      ▶<exclude-controls with-child-controls="token"> … </exclude-controls> [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
                   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:

```yaml
- 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

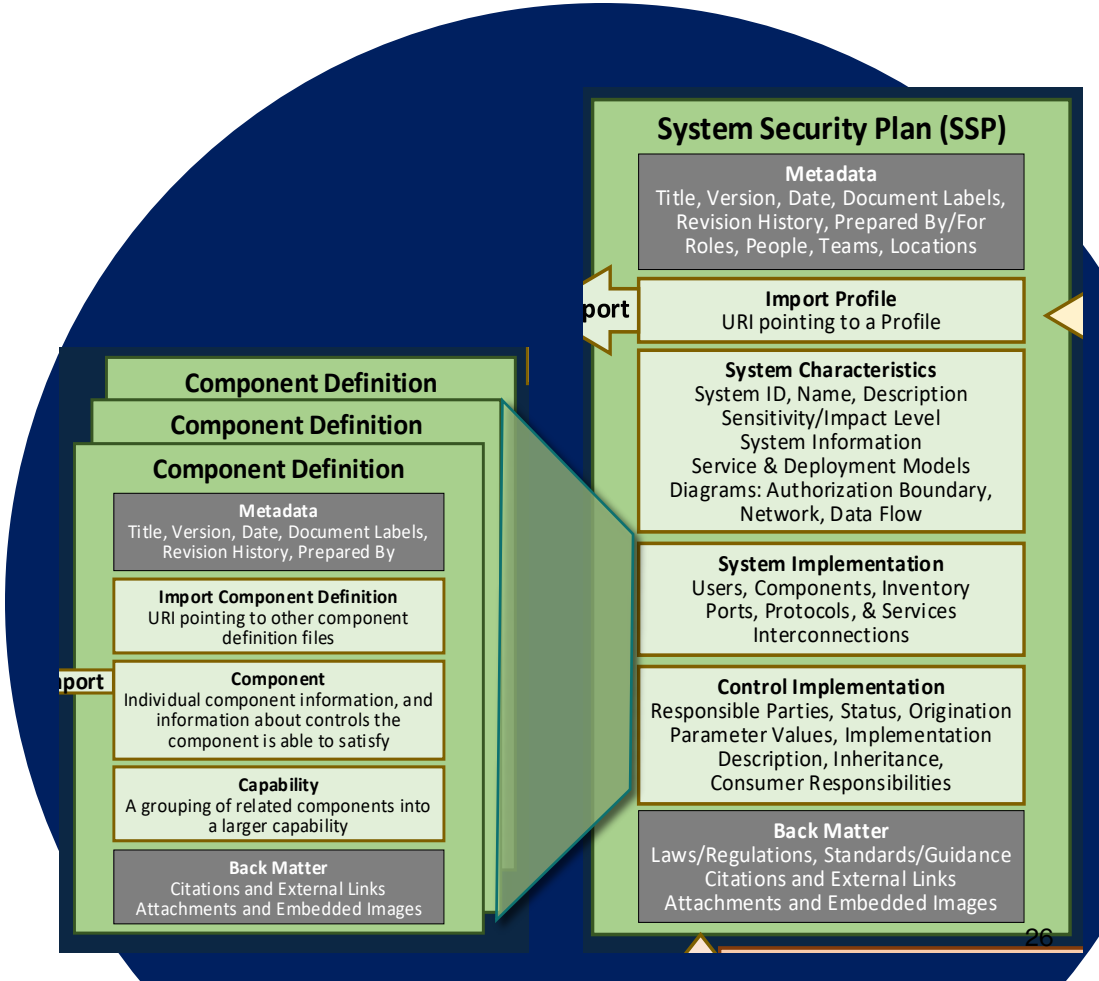
```
</control>
 <control class="ssc-iso-sc27" id="s6.1.2">
  <title> Séparation des tâches</title>
  <prop name="label">6.1.2</prop>
  <prop name="sort-id">c02</prop>
  <part id="s6.1.2_stm" name="statement">
   <prop name="label"> Mesure</prop>
    <p>Il convient de séparer les tâches et les domaines 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

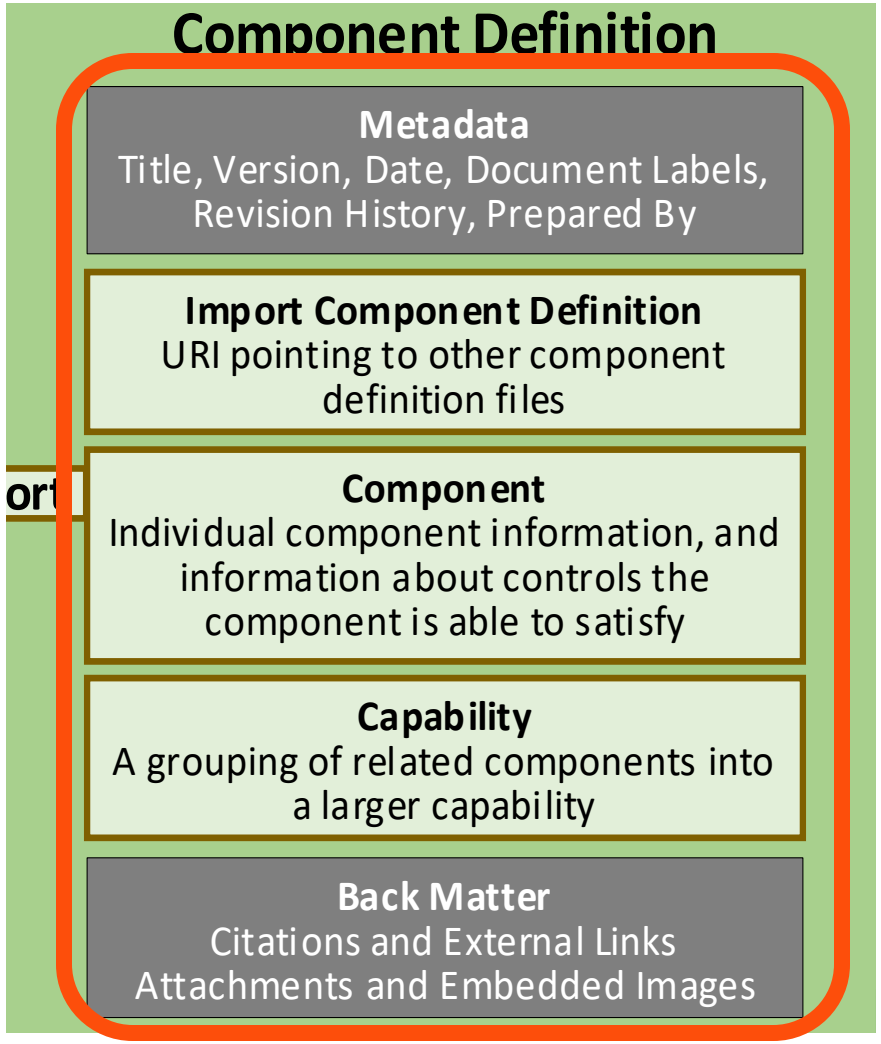


The Component Definition ...

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

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

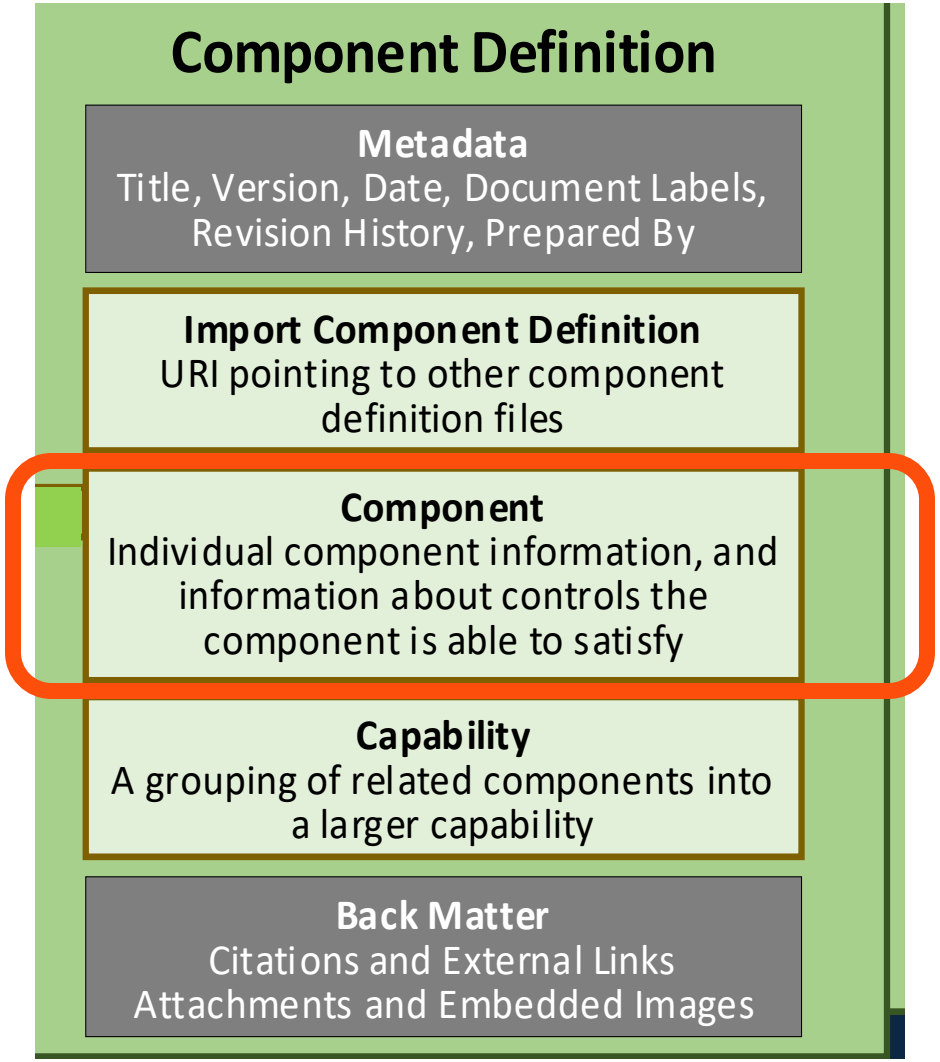
```
▼ component-definition [1]: {
      uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▶ import-component-definitions [0 or 1]: [ … ],
    ▶ components [0 or 1]: [ … ],
    ▶ capabilities [0 or 1]: [ … ],
    ▶ back-matter [0 or 1]: { … },
  }
```



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,
            }
        ],
    }
],
```



Cybersecurity ‘Shipping Container*’

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

OSCAL Component Definition Model allows:

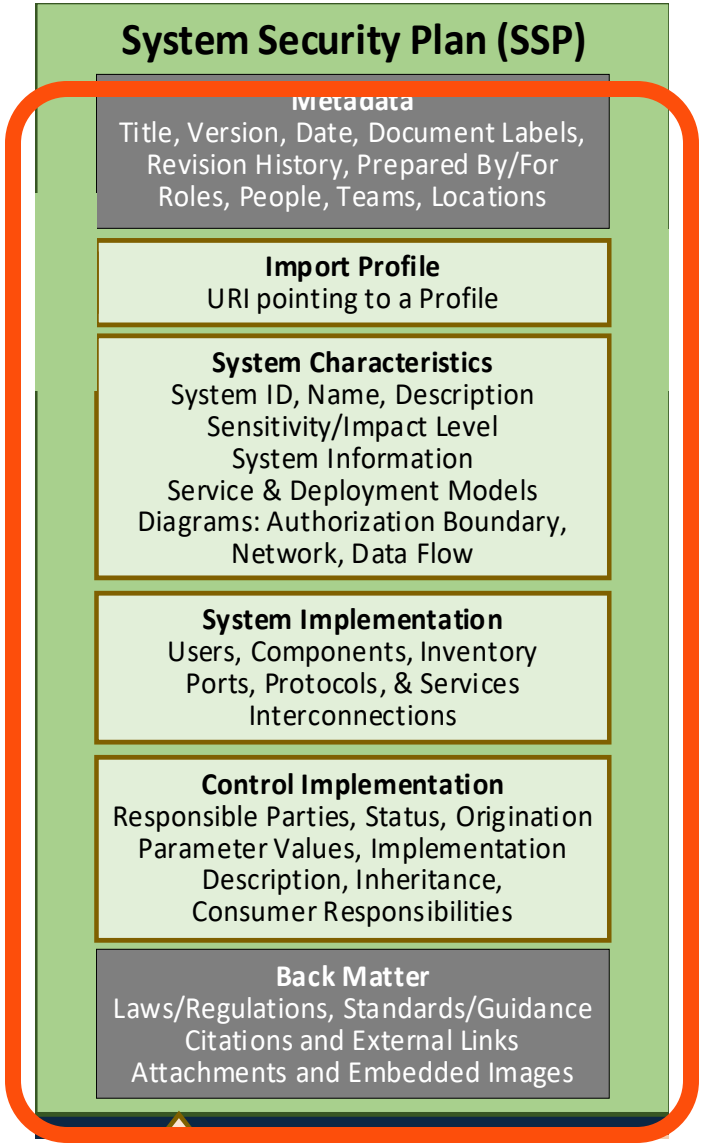
- ❑ Vendors to document the security controls implemented by their products
- ❑ System owners or policy makers to define ‘playbooks’ for system components
- ❑ System owners to test, review and provisionally authorize system components
- ❑ Reuse the components for different systems
- ❑ Ease the system’s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

*Courtesy of a collaborator requesting anonymity.

The SSP Model

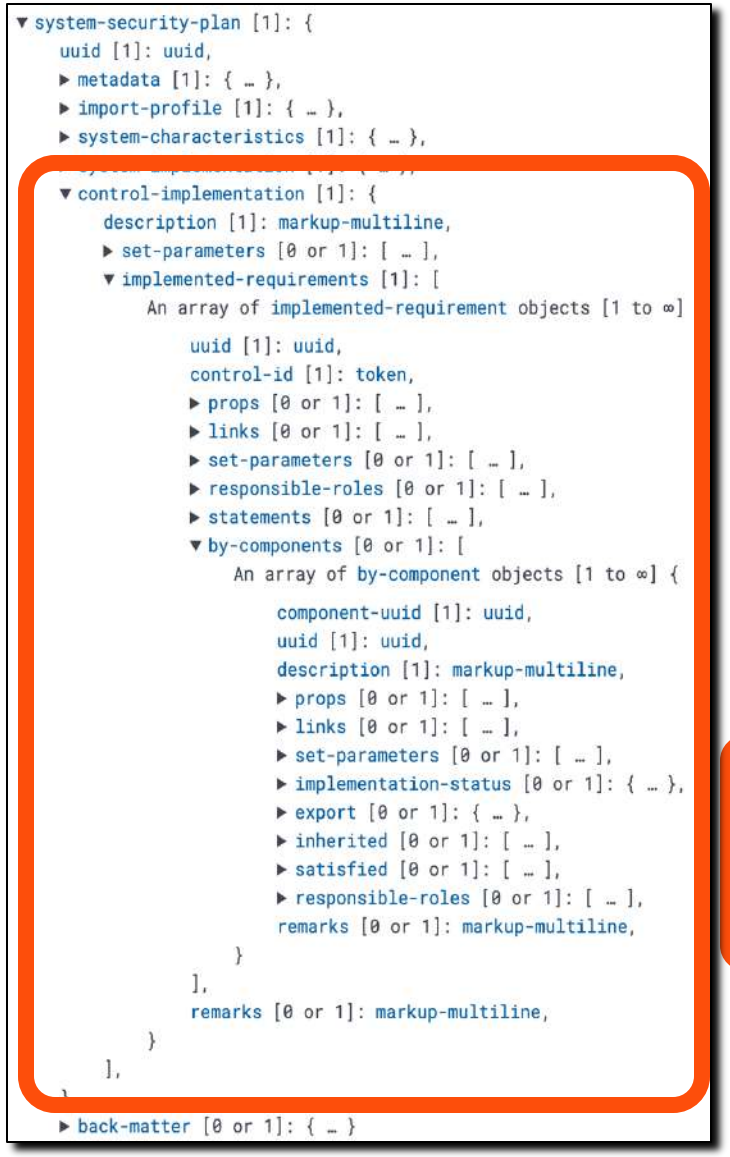
https://pages.nist.gov/OSCAL/reference/latest/system-security-plan/json-outline/

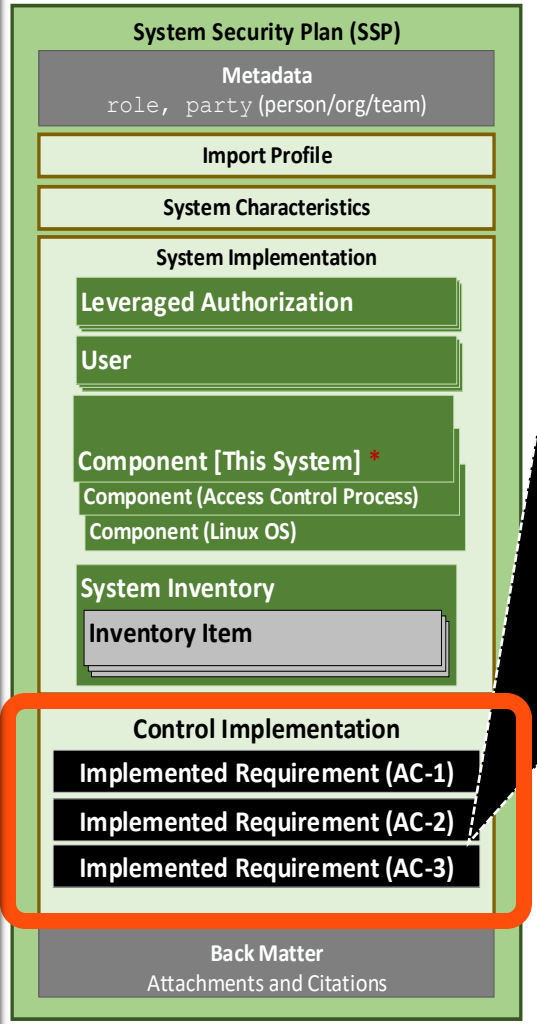
```
▼ system-security-plan [1]: {
    uuid [1]: uuid,
    metadata [1]: { … },
  ▶ import-profile [1]: { … },
  ▶ system-characteristics [1]: { … },
  ▶ system-implementation [1]: { … },
  ▶ control-implementation [1]: { … },
  ▶ back-matter [0 or 1]: { … }
}
```

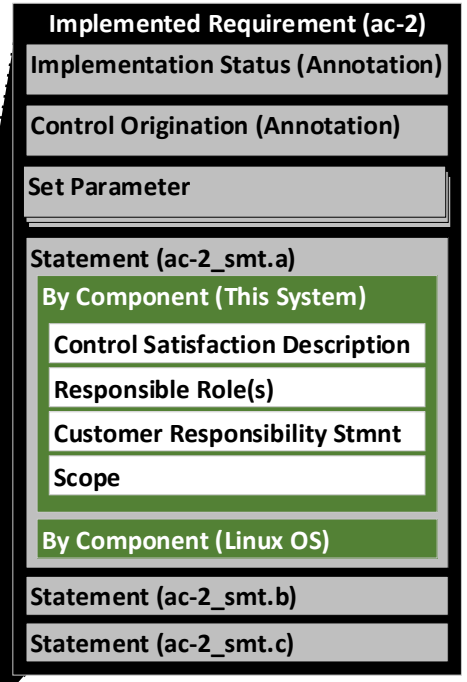


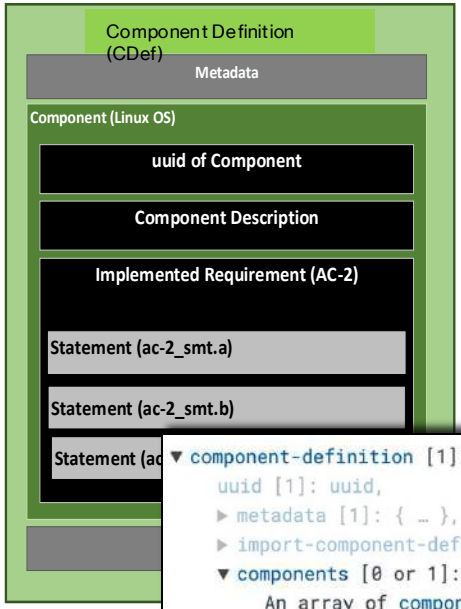
The SSP Model ...

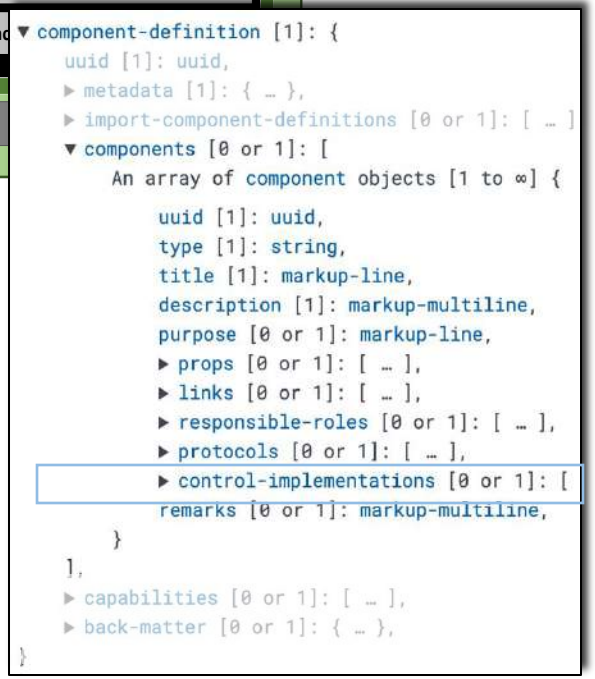
https://pages.nist.gov/OSCAL/reference/latest/system-security-plan/json-outline/











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!

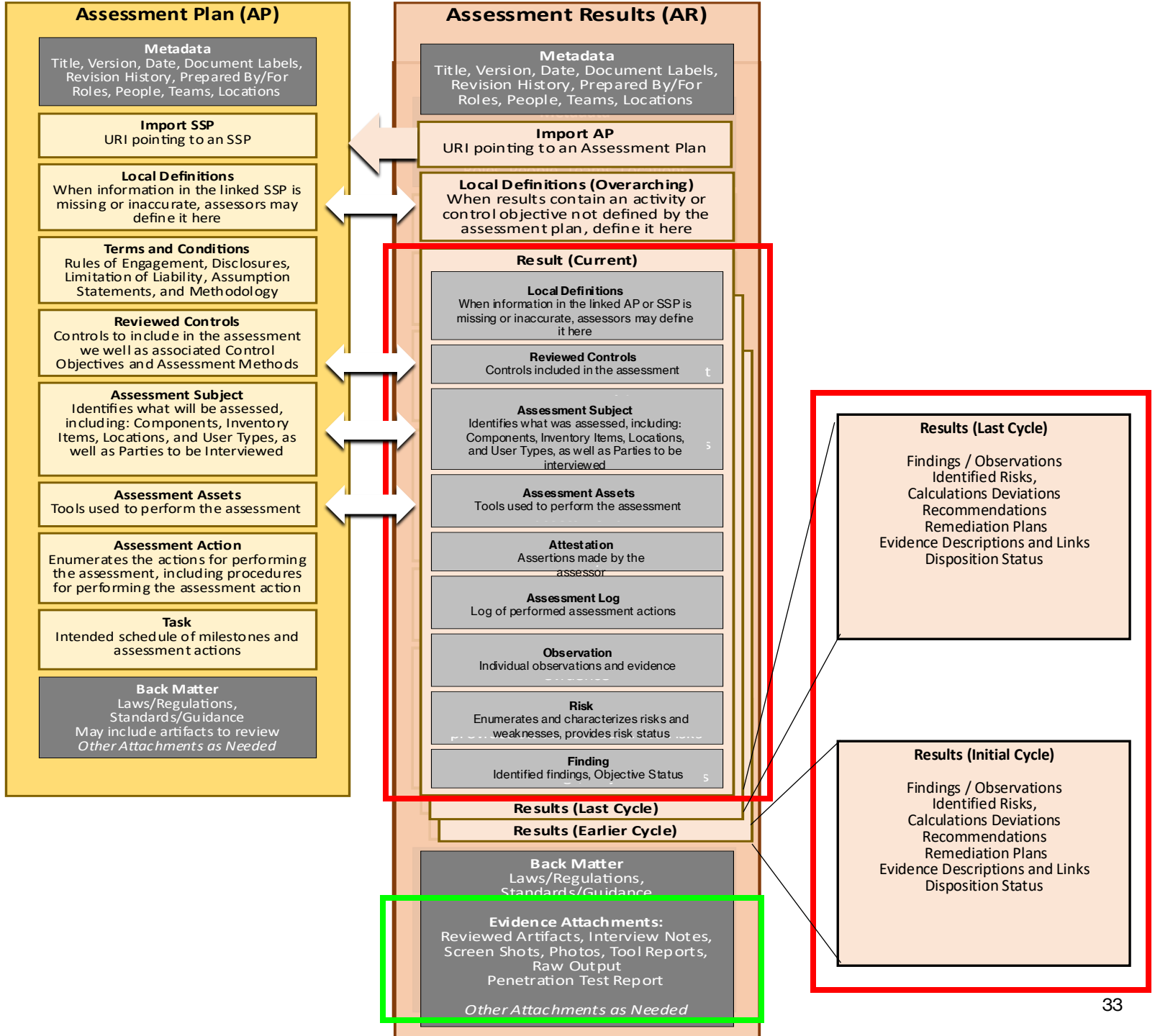
- Review the components in the context of the respective system
- Review the interaction between components
- Get the max return in your investment – be granular with the data and the assessment

Assessment Plan (AP) & Assessment Results (AR)

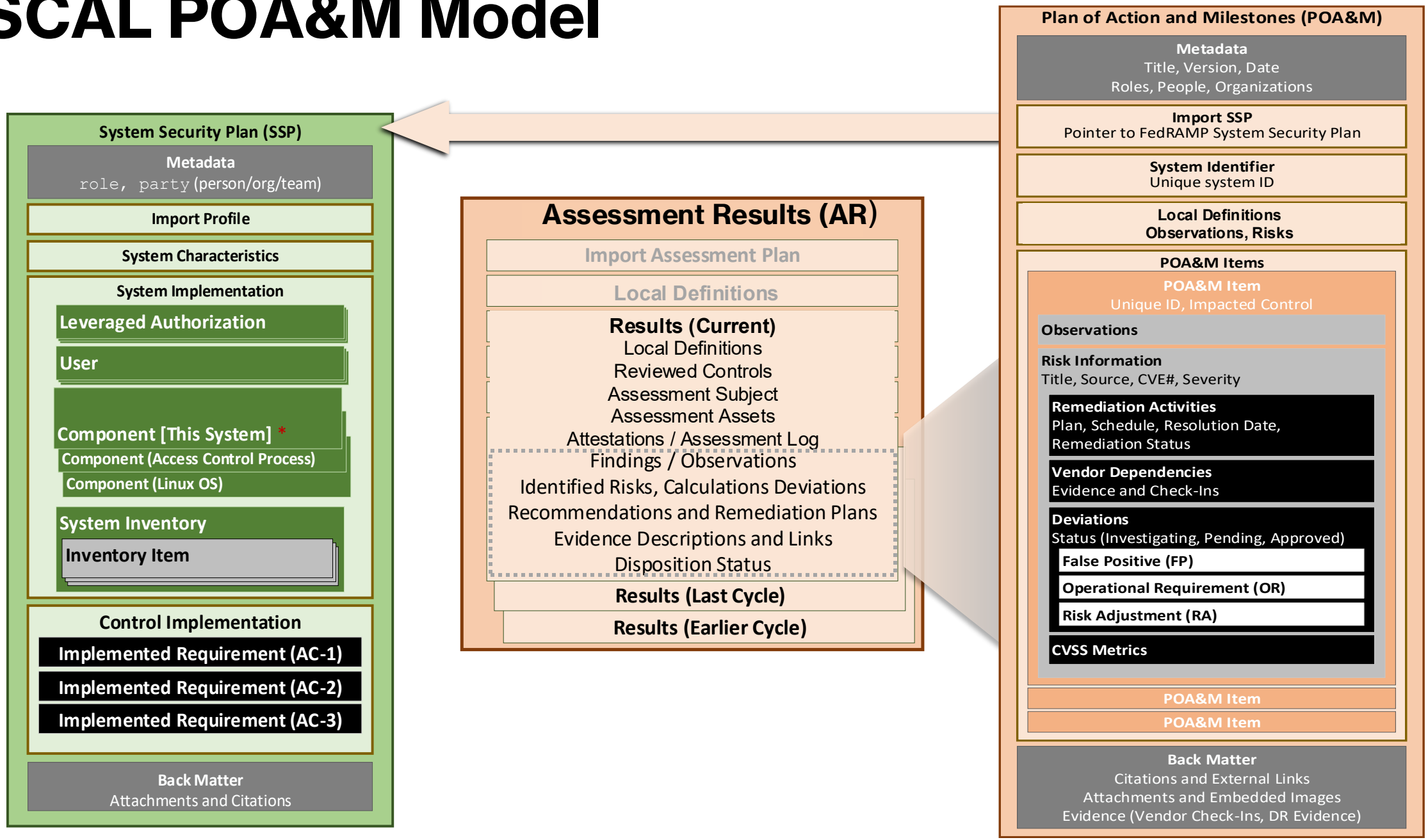
- ❑ Overlapping syntax
- ❑ Similar but distinct purposes
- ❑ **Unique to AR**: Results and Evidence

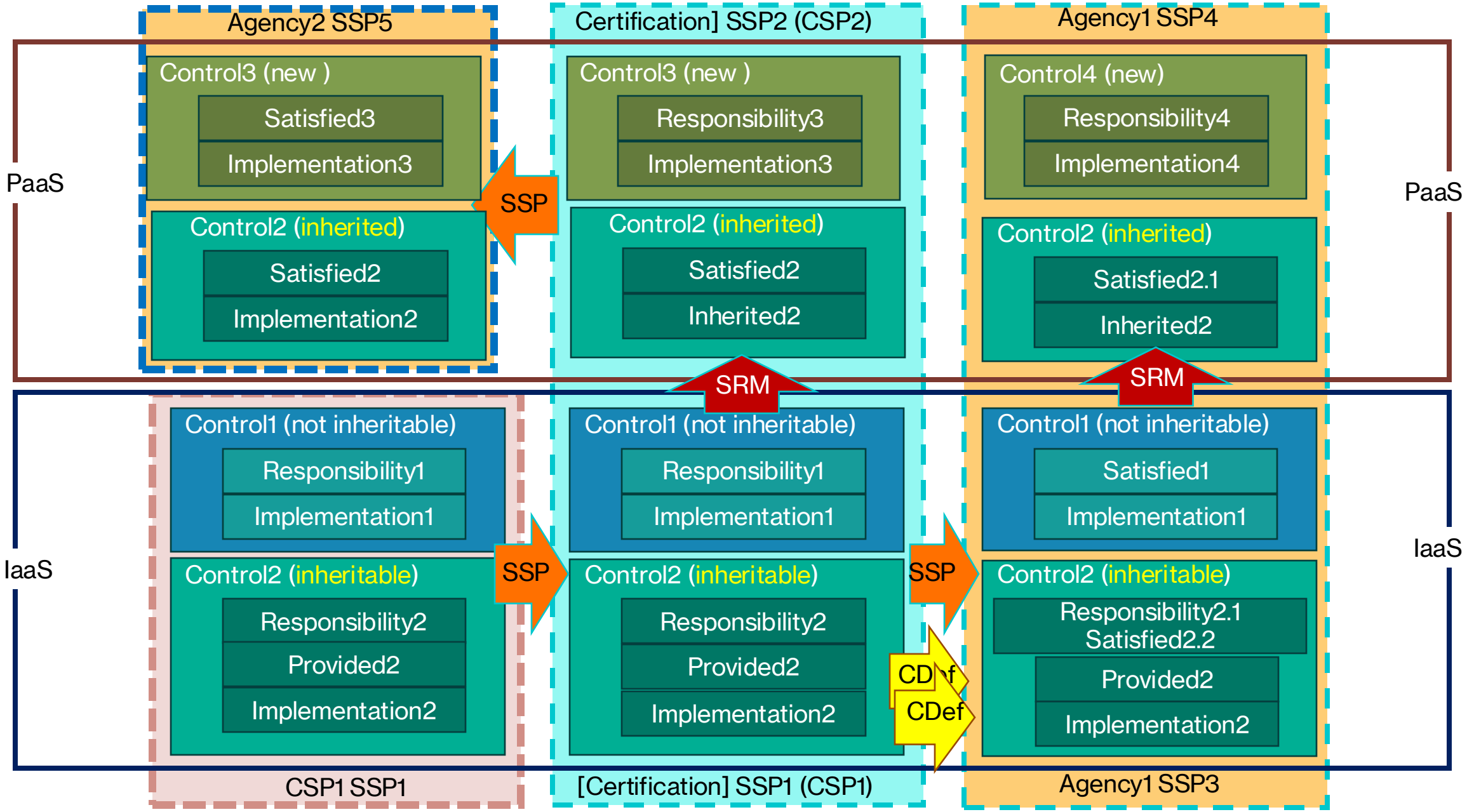
Continuous Assessment Approach

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

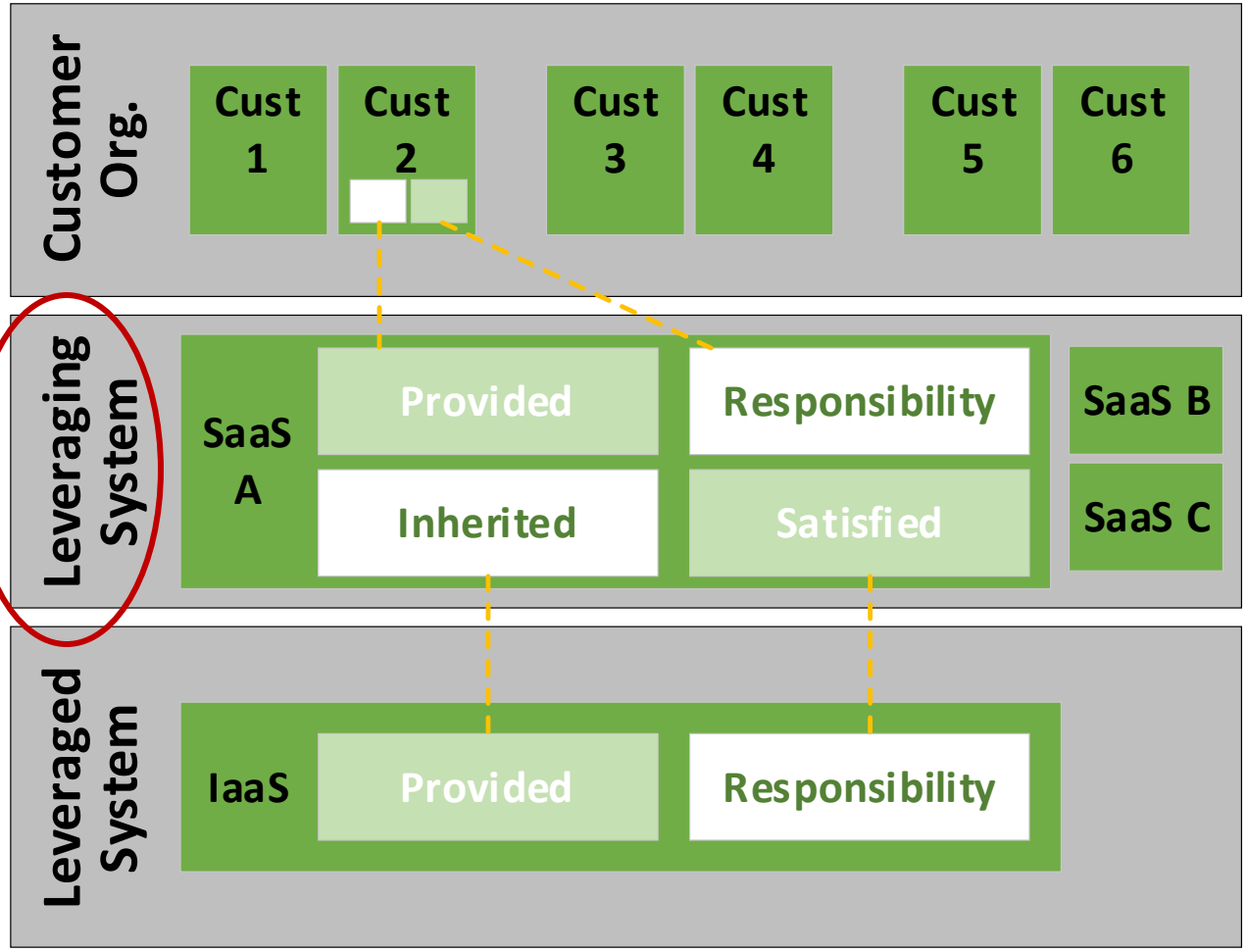


OSCAL POA&M Model




Agency2 SSP5
Control3 (new)
Satisfied3
Implementation3
Control2 (inherited)
Satisfied2
Implementation2
SSP
Certification] SSP2 (CSP2)
Control3 (new)
Responsibility3
Implementation3
Control2 (inherited)
Satisfied2
Inherited2
Agency1 SSP4
Control4 (new)
Responsibility4
Implementation4
Control2 (inherited)
Satisfied2.1
Inherited2
PaaS
PaaS
SRM
SRM
Control1 (not inheritable)
Responsibility1
Implementation1
Control2 (inheritable)
Responsibility2
Provided2
Implementation2
SSP
Control1 (not inheritable)
Responsibility1
Implementation1
Control2 (inheritable)
Responsibility2
Provided2
Implementation2
SSP
Control1 (not inheritable)
Satisfied1
Implementation1
Control2 (inheritable)
Responsibility2.1
Satisfied2.2
Provided2
Implementation2
CDef
CDef
IaaS
IaaS
CSP1 SSP1
[Certification] SSP1 (CSP1)
Agency1 SSP3

The Shared Responsibility (SR) Model

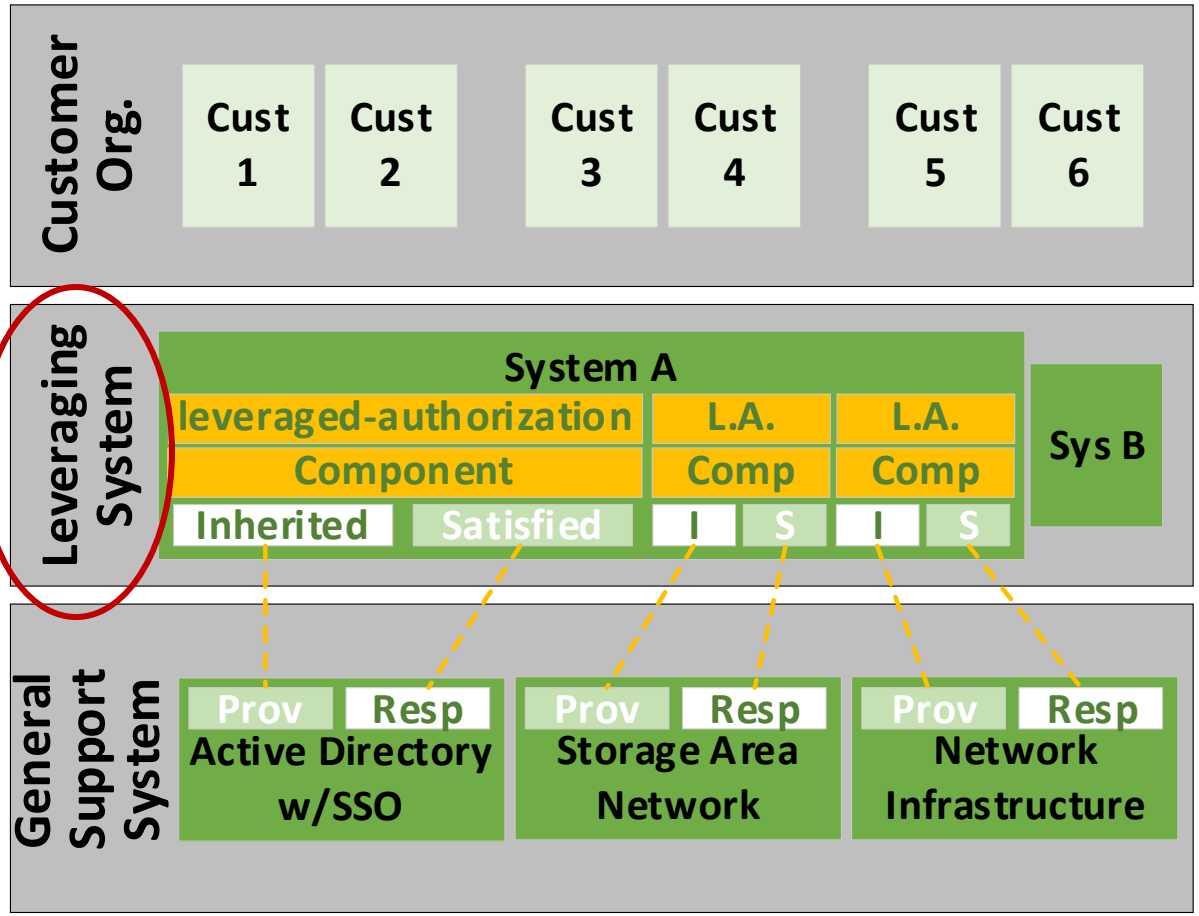


- **Leveraging System:**
- The leverag**ing** system's SSP should:
  - identify what is inherited from a leveraged system
  - identify any addressed responsibilities (as identified by the leveraged system)

In addition to:

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

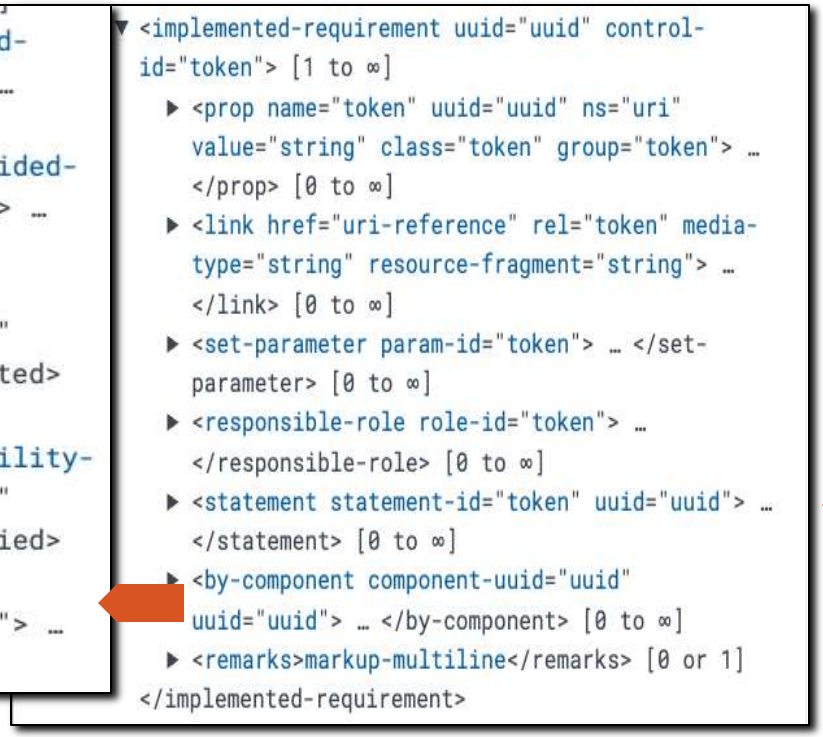
Multi-layer SRMs ...

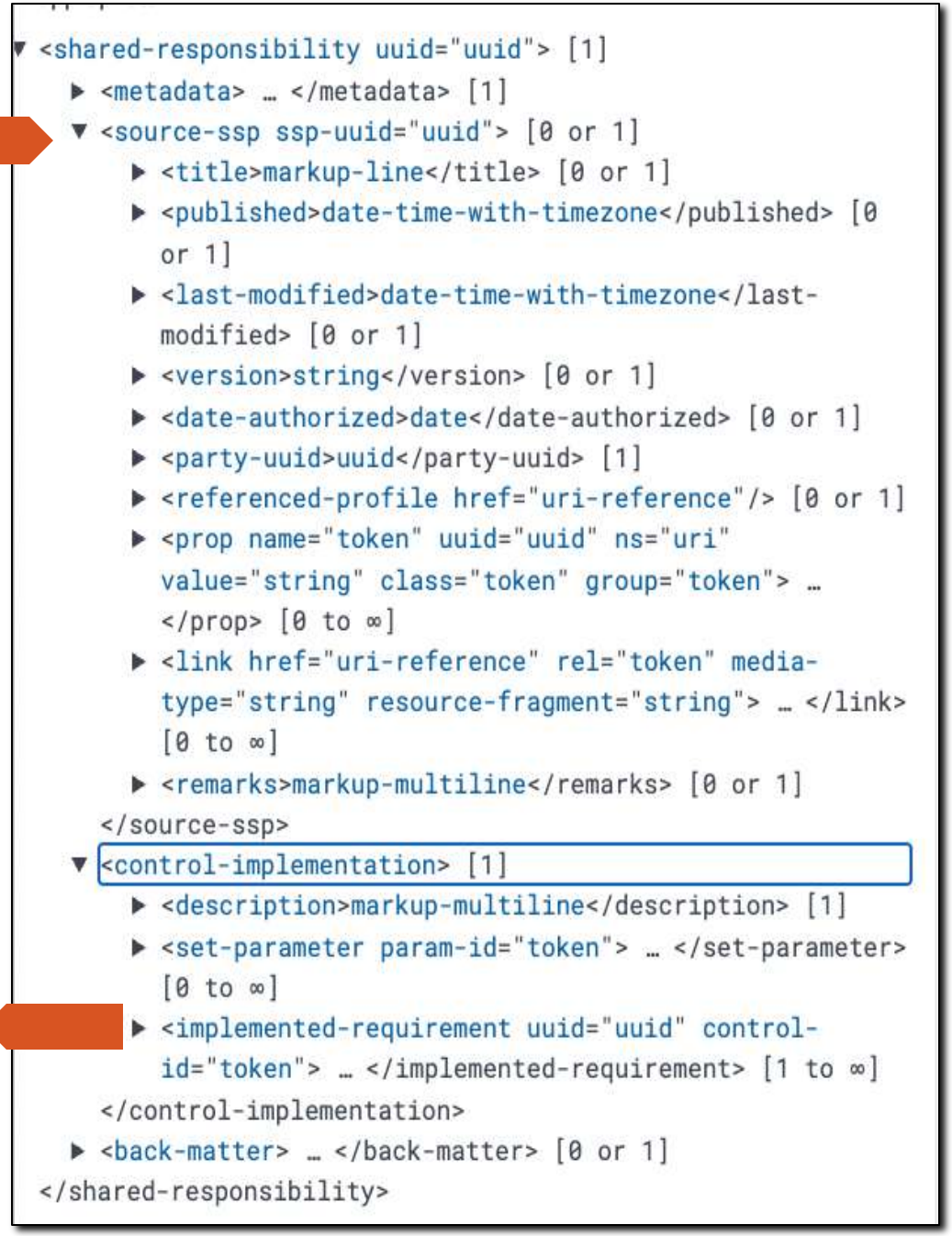


- **The same syntax is used**
  - It is simply replicated for each leveraged system
- **The Leveraging System's SSP:**
  - Has a separate "leveraged-authorization" assembly for each leveraged system.
  - Has a separate "component" representing each leveraged system.
  - Has a separate "component" representing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

The Prototype Shared Responsibility Model

- Outline -



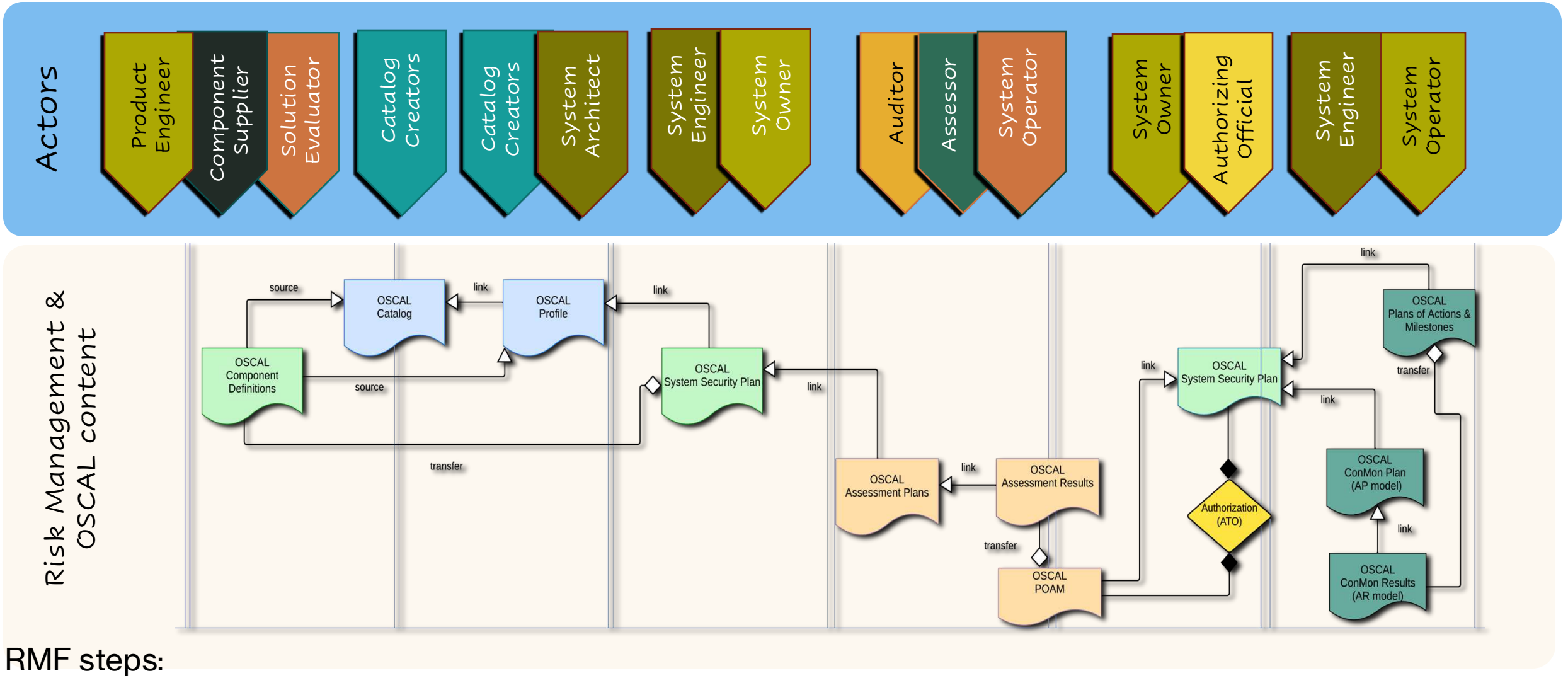


The Prototype Control Mapping Model

- 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

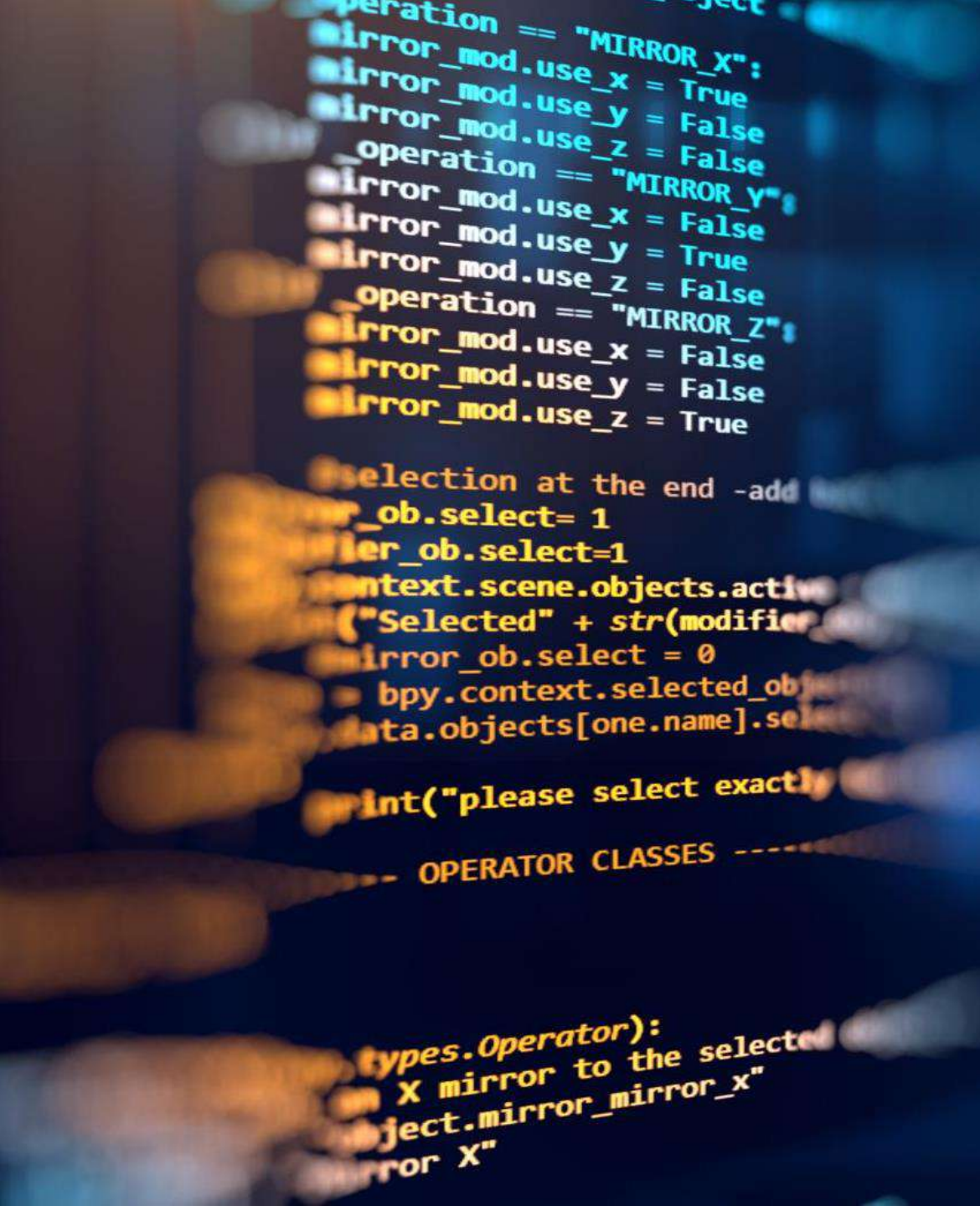


RMF steps:

PREPARE CATEGORIZE SELECT IMPLEMENT ASSESS AUTHORIZE CON-MON

OSCAL Adopters Around the Globe

The future of OSCAL ...



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

THANK YOU !!