

From Digital DNA to Digital Immunity

with

OSCAL

Open Security Controls
Assessment Language

Dr. Michaela Iorga,

Director, OSCAL Program, CSD/ITL/NIST

July 16, 2026

Agenda

- ☐ IT modernization calls for automation.
- ☐ What is OSCAL.
- ☐ Continuous risk management with OSCAL.
- ☐ OSCAL-driven system resiliency.
- ☐ What is next.



NEW MAJOR DIRECTIONS & CYBERSECURITY EVOLUTION

EO 14306: Sustaining Select Efforts to Strengthen the Nation's Cybersecurity (June 6, 2025) (amends earlier EOs)

- ❑ directs NIST to update *NIST SP 800-53* guidance on secure patching, software development, and AI vulnerability management.
- ❑ directs pilot programs for machine-readable policy ("rules-as-code")

EO 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity (2025/2026)

- ❑ reduction of regulatory burden through automated controls assessment
- ❑ evolving software security reporting protocols

EO 14179: Removing Barriers to American Leadership in Artificial Intelligence (Jan 23, 2025)

- ❑ strengthen U.S. AI leadership by revising or rescinding policies seen as impediments to innovation

FISMA (Federal Information Security Modernization Act (2014)

- ❑ agency-wide information security programs
- ❑ periodic assessment of the risk and magnitude of harm ...

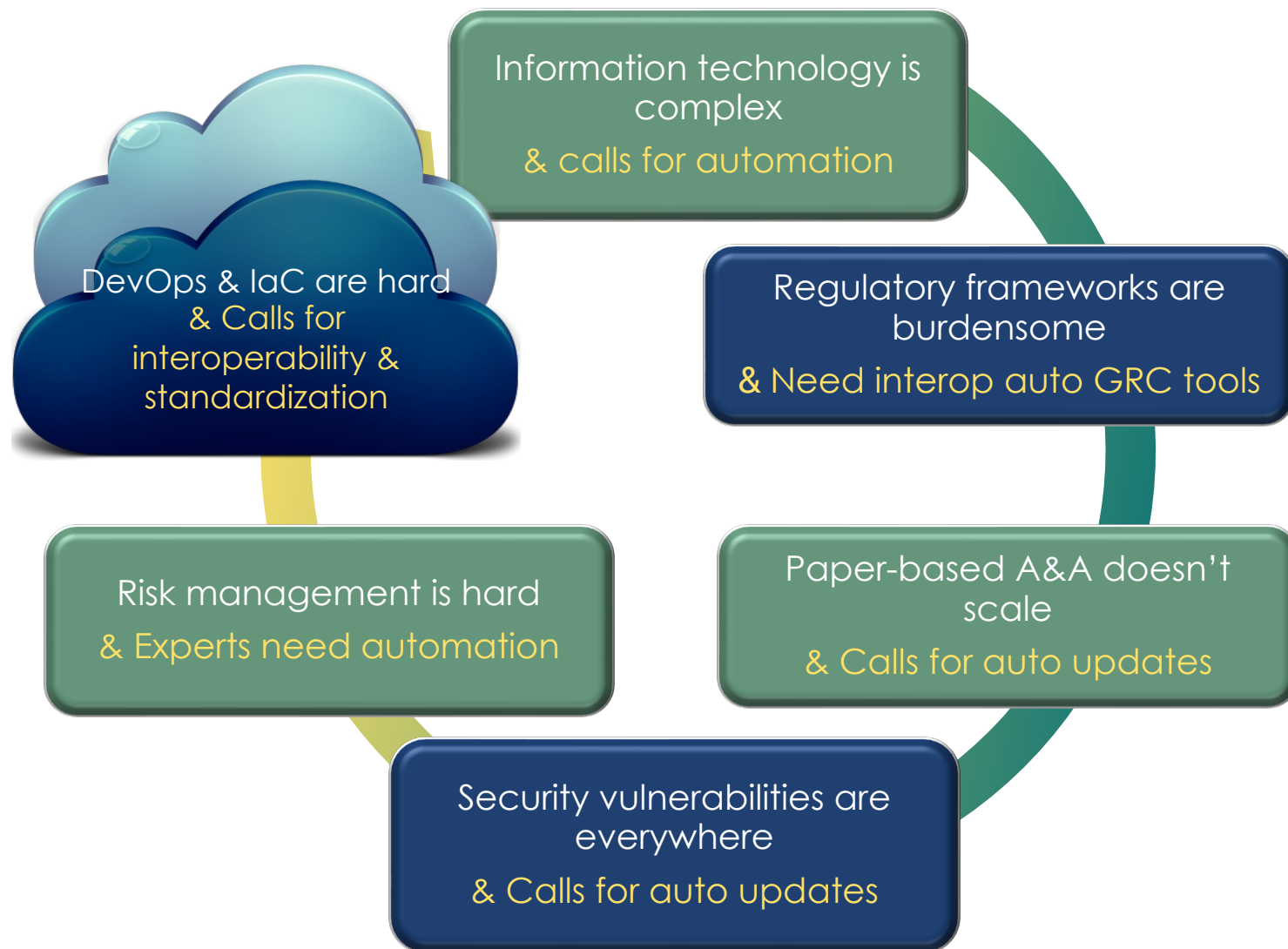
The Struggle...

PERIODIC ASSESSMENT
OF THE RISK &
MAGNITUDE ...

Before the audit

During the audit

After the audit



Cloud Means Automation! Then Why is it Hard?



- ❑ Cloud service providers and tool vendors rapidly developed innovative solution to automate system scanning and monitoring.
- ❑ What is provided is not always what is expected by cloud service consumer
- ❑ Consumers and providers might have different risk tolerance levels
- ❑ Documentation is never up to date, dashboards showing de facto security posture but not the risk mitigated one.

Open Security Controls Assessment Language

OSCAL is a framework that defines open, machine-readable data models for security controls, implementations, and assessments.

OSCAL Layers:

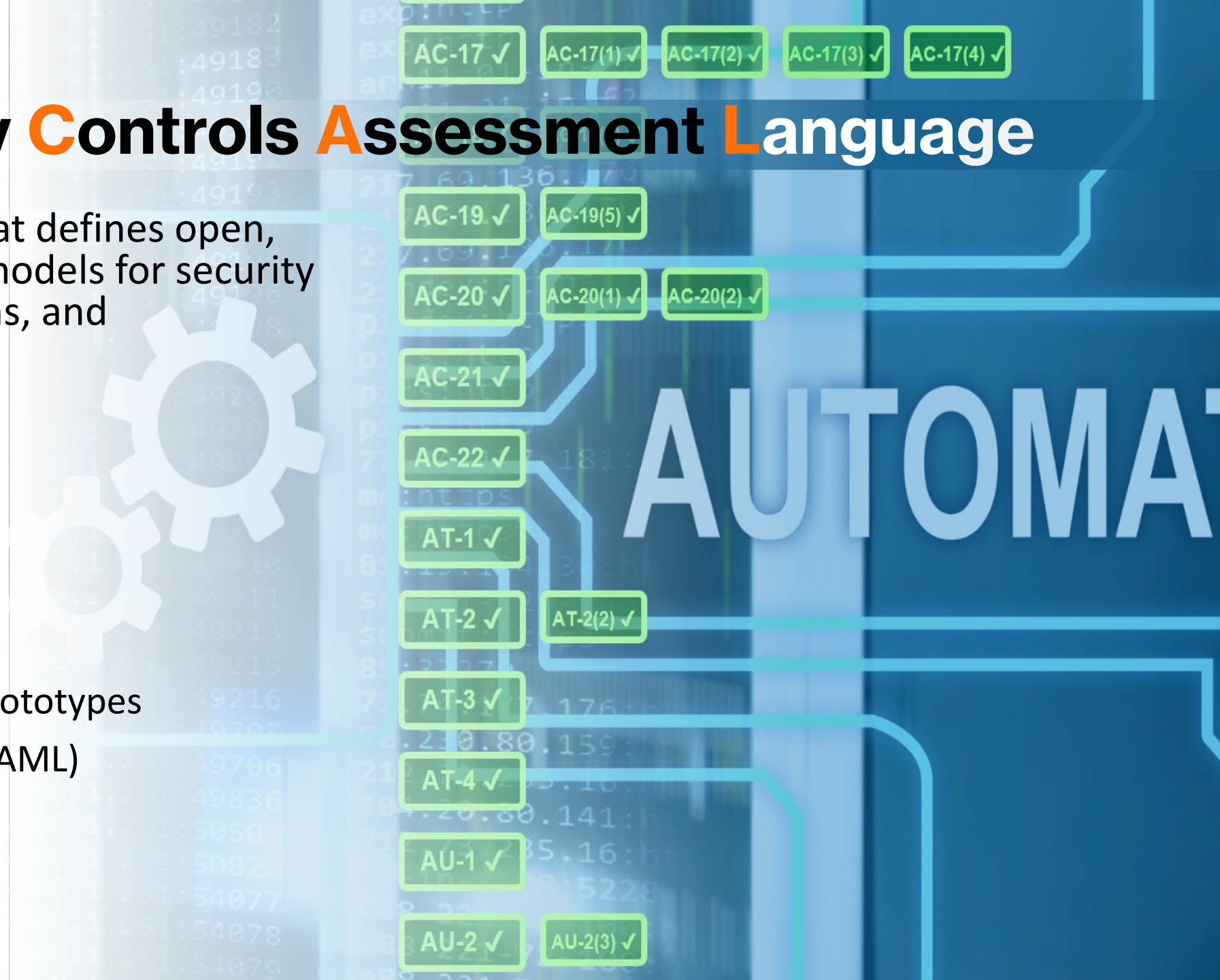
- Control (What)
- Implementation (How)
- Assessment (Proof)

Currently Supports:

- Models: 8 released + 1 prototypes
- Formats: 3 (XML, JSON, YAML)

Future State:

- ISO/IEC Standard



Spreadsheets, Excel, Google Sheets and the Standardized Schemas Behind

```
PK!Ôáàà[Content_Types].xml 4(†"TÖN1æð-ð^
[â`âa0ÄzT0J;∞
>ðÈ
o0lQb
≤!Ôeð>væüô07æfl6Æÿ@B|FÂP±u0÷/+0>{<äIyflâPâ†ü^âgâXpµ«J'D
ÀiÜE"$F0¶•âJ0'‰1px#uâû'bà...jÎ@x<ÚÁΩíπ1çð0æµTîP1:±Pπ0Ê...
bc(%Qæ#~rUreÜµcx≈÷`hw_v1U~„H÷@0™='Ü0Ä≈i!≠Ê!" Á&Σ@lî
"Æ">^
/≈\`Êç^-.{â^Ájæê'.}è=ÉvâkÂÛ¥Ê+/ÜΠβ^-9R^Sà»©i‡|fl-V"A"
áê8^≥9Ú.î/L5`épÄú.î0~PK!µU0#ÜL
_rels/.rels 4(†"íM0v0
Ü0H_á»~'>èBKwAH^!T~ÄI<µçf$>ø'TÉGΩ~ €><çÍ»!^,4"ã;#ðw≠Üó`q
fl#F"0D±æ.W •Ü=ôÂZΔMYfib~Æ'BSÏ≠Ü∞Σ7†Îìæðñ¶È
?à9Lî"ô>sbgÿÆ|»l!~USH9i∞bûr:"y_dlîÜDðø~|~Nú»R"4~2æG«%†1Z
xl/workbook.xml`V[of8~_i`ãÊîçôâHmv"6Jðv~)ri VndlßI5ö`æ«&4
„¥©áfuai©≥&ß1f@Iv∇5.pù„≤©...P"\"<'1óÄ}~V0ðÉAÄö1BàmÄæ
Ra~lI
#ÎÜUX@imfl2Çs^"™Y¶È°
"ZovF≥^"âDMâ`H-ZFJ,Ä>/ËñwhUv\ÖÿvñkdMµà{ZR0$@u≠ ÇÈ¶næ/iîÉÄ
Y÷+fi`†<$1ÚHÄ>≥bfiYyæXfi Ä2Öi)≠†çµæ<l}tπ¶%πm•`·Î^WÚ$J]+1qN...
VZP~w`πÆ.ùh&†F8ü"LI†a@ðr5â%,a5d"¥y¥1gu@'E™◇%Îé™MAS`?i8
â=üçQh;VuÜ0ÉCPE!†0ä0Ö≥ÿjæ¶~#ú$K002æN√tzsQ`
≠¥öÄ$úÄÜmæHIV$
◇|Mz!r_>ç.ÉÄq&~NîQ≠1îÜ[BÂM,Ë$<LÉÁi4É,,\,G8\êP~â")úúø`Ê≈ð„Z
B?6æ~fl
]°;Xið k†âf`$ÊPw@0ÜÆâ±Ä`GÜ".flÄ„«é1ðç°.-i©0ñí=?IK6µv≠Üf<
|Ëÿ`·;öâb@ÆwÍ`ù-Mú≠ûo Pbð%6`_qäZN
Yº,N^êRi»©Z`UË$·Úæ%$§{ð°•{-àî@nî¶π
'≠ ...ð÷$óQ/ZG$'°`'â9fµX•Tîpi@f¶\vÿ¶>R€`^...>ÿóÊH„5>~Àd\B•h
j"...% f\@%0iñcÜ}s†f<s
«ÿÜ0Ä:&Nd«n?é,±+Ä Ô`†~»<×
É02î,Äf0^WËÇ`«ðÉp[~flód«Æ?6{@-I";0ç0ÿs
7Jznflä&±ðú»JÜ0Äö>R` VIK¶'dô{ü;◇m«0(≈x∞â$flè`~m,"/...
ôîi€3'NÆ0"~3ÄE,tuóú:9ºG•`Üv≈";ç`Îâ@?t(zs†}◇0≈n'3l7Ë°ð^†N
Qyç`æ≠p°dDQR~Î`<á dY1ç¥$f¶ßlî!IK≈
Ít;`~PK!íîî?xl/_rels/workbook.xml_rels 4(†"íÄjF0
E~0_É-æq2}PÛqf-Ròmð~Äpî8Lb[}%0kR:...îên≤1H~ââ€w≠$gdI
C`veck0≈Ä0#àîhKlù%ÿÄ◇WªWjê„B`ö>à@bÉv<o•
/Pá!q=ÿ8©ú0êcÈkÿf>bMrî¶"æ5 ?"áRÄ?îΣ ä°èÆ`kæ™j4=;~-ëÄ
```

AutoSave



Home

Insert

Draw

Page Layout

Formulas

Data

Review

View

A



Paste







Calibri (Body)

11

A⁺

A⁻

B

I

U







Genera

\$

L11

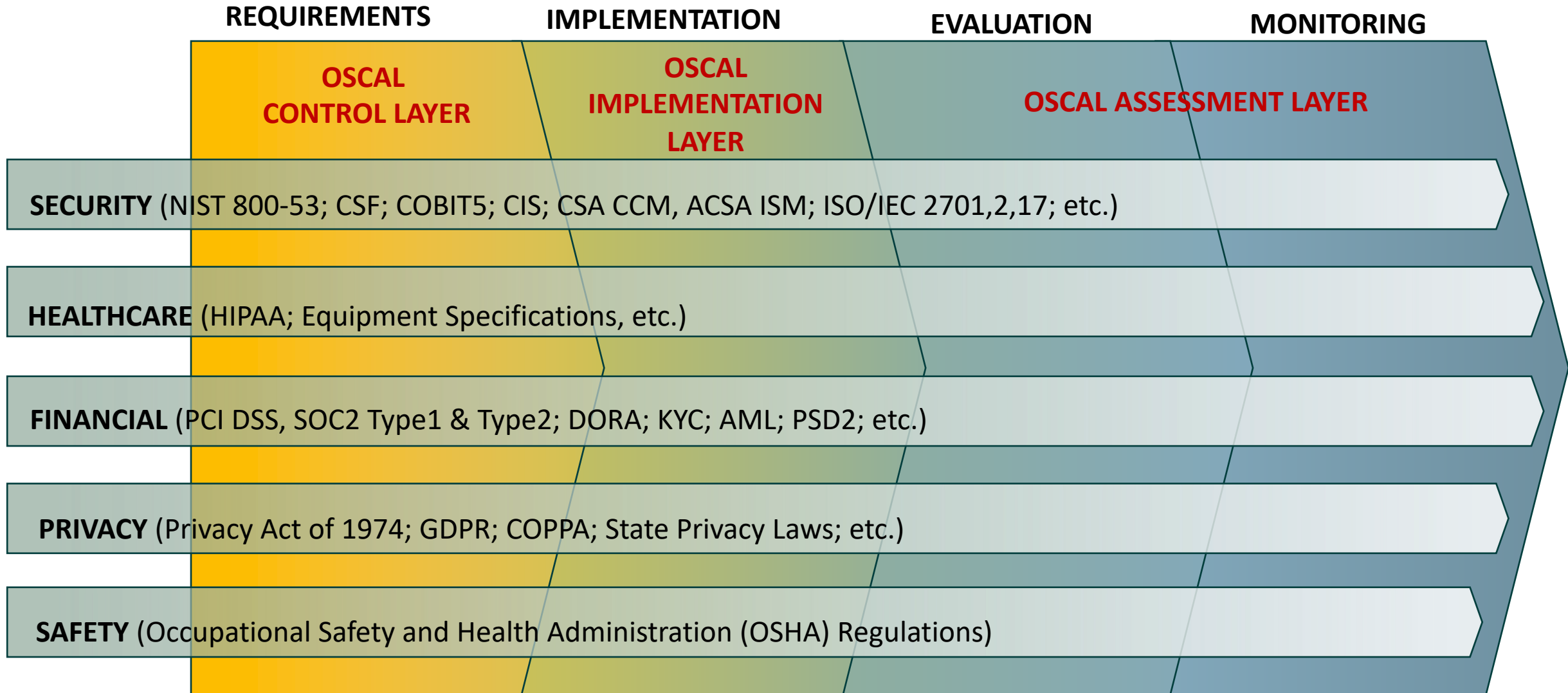
<

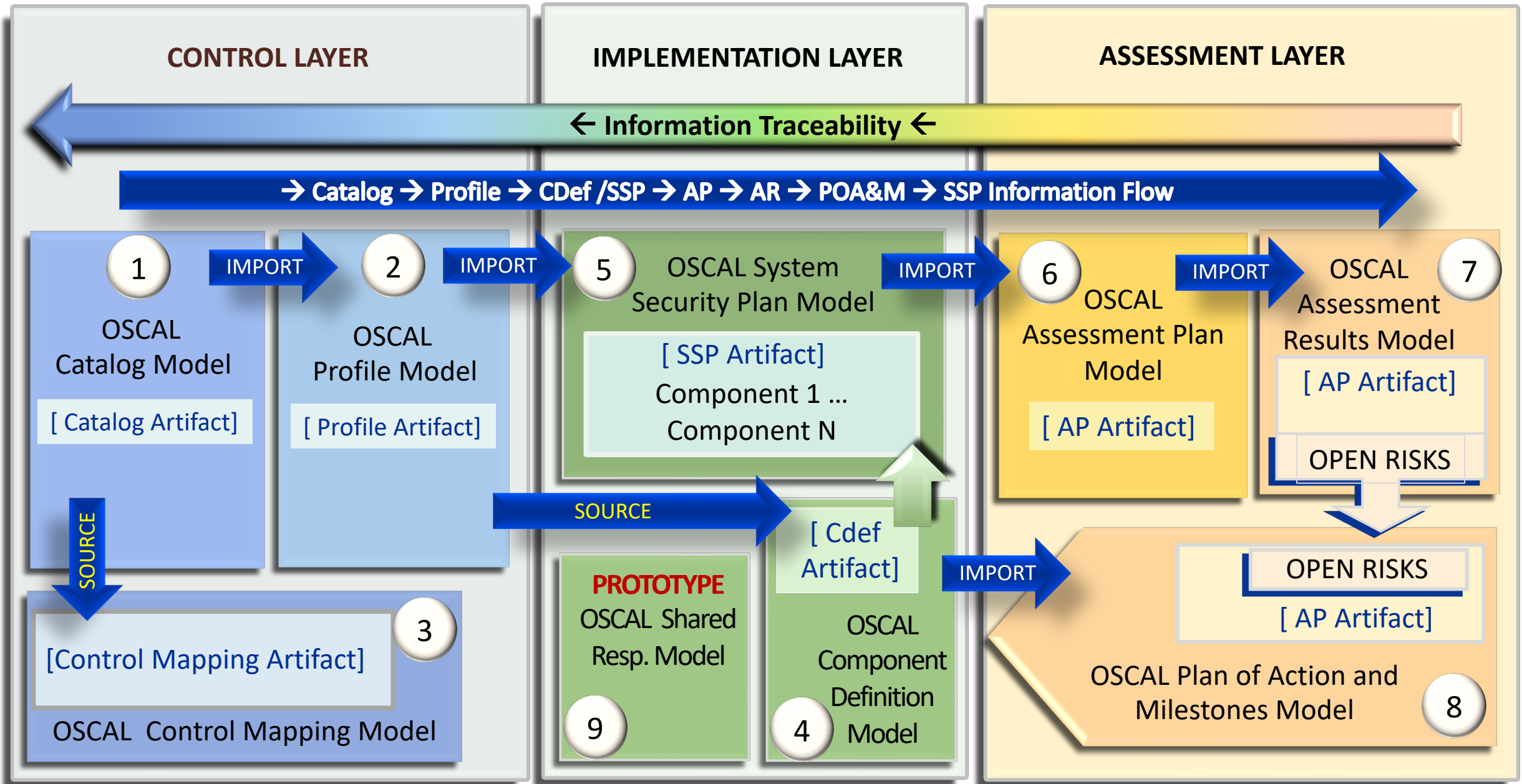
Design Goals ...

- ❑ Improve the **efficiency, timeliness, accuracy, and consistency** of system security assessments
- ❑ **Enable traceability by design** from the implementation and assessment back to the original control statements
- ❑ Set the **foundation for automation and interoperability**

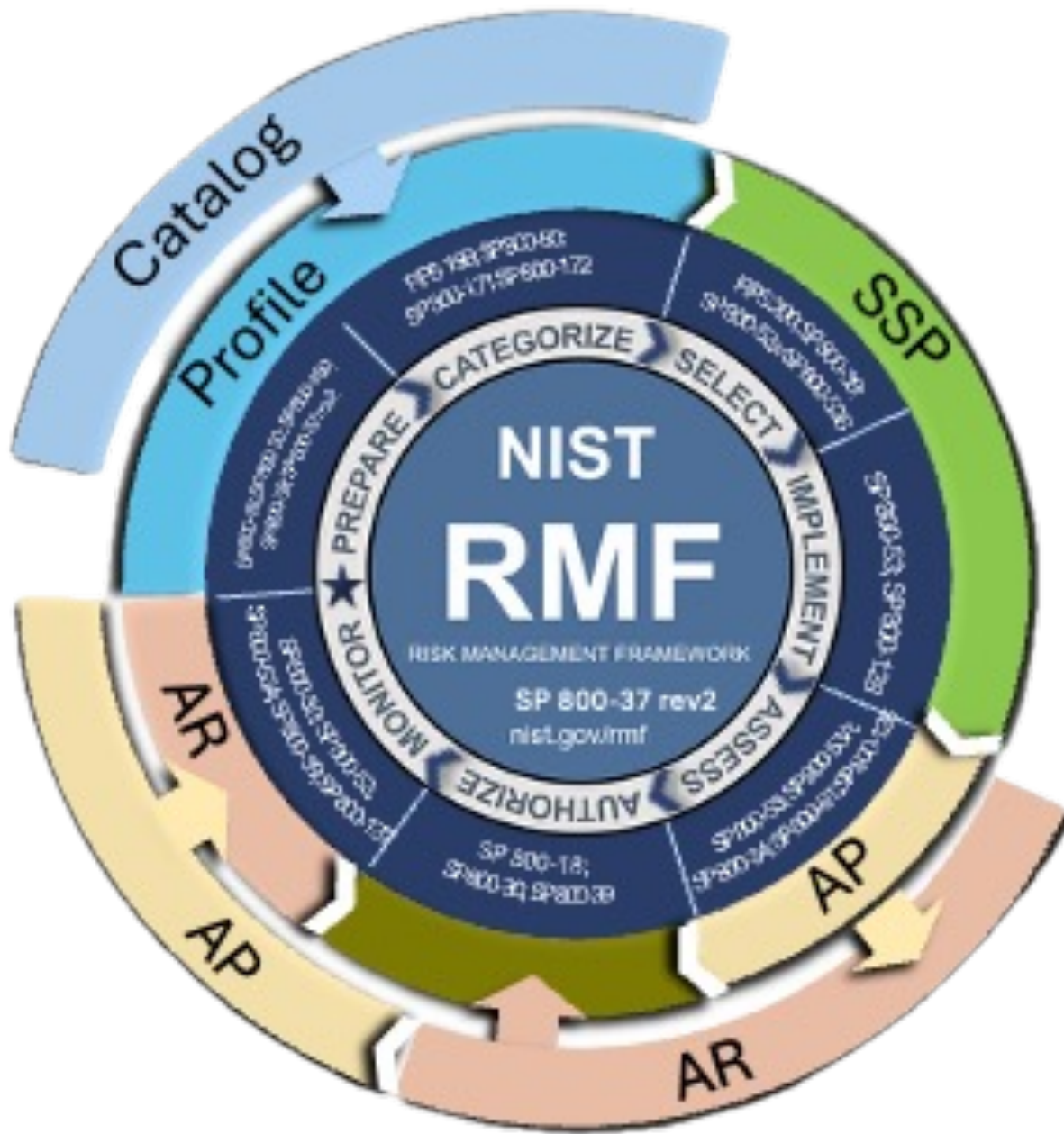
- ❑ **Open** ➤ **Free** for everyone
- ❑ **Security** ➤ **Not only** (security, privacy, safety, etc.) => **S**andardized (?)
- ❑ **Controls** ➤ **R**equirements that need to be implemented and the implementation be assessed
- ❑ **Assessment** ➤ **E**valuation of the safeguard implemented in response of a set of requirements
- ❑ **Language** ➤ **D**igital representation – a translation of the information for machines to consume.

Applicable to Any Domain ...



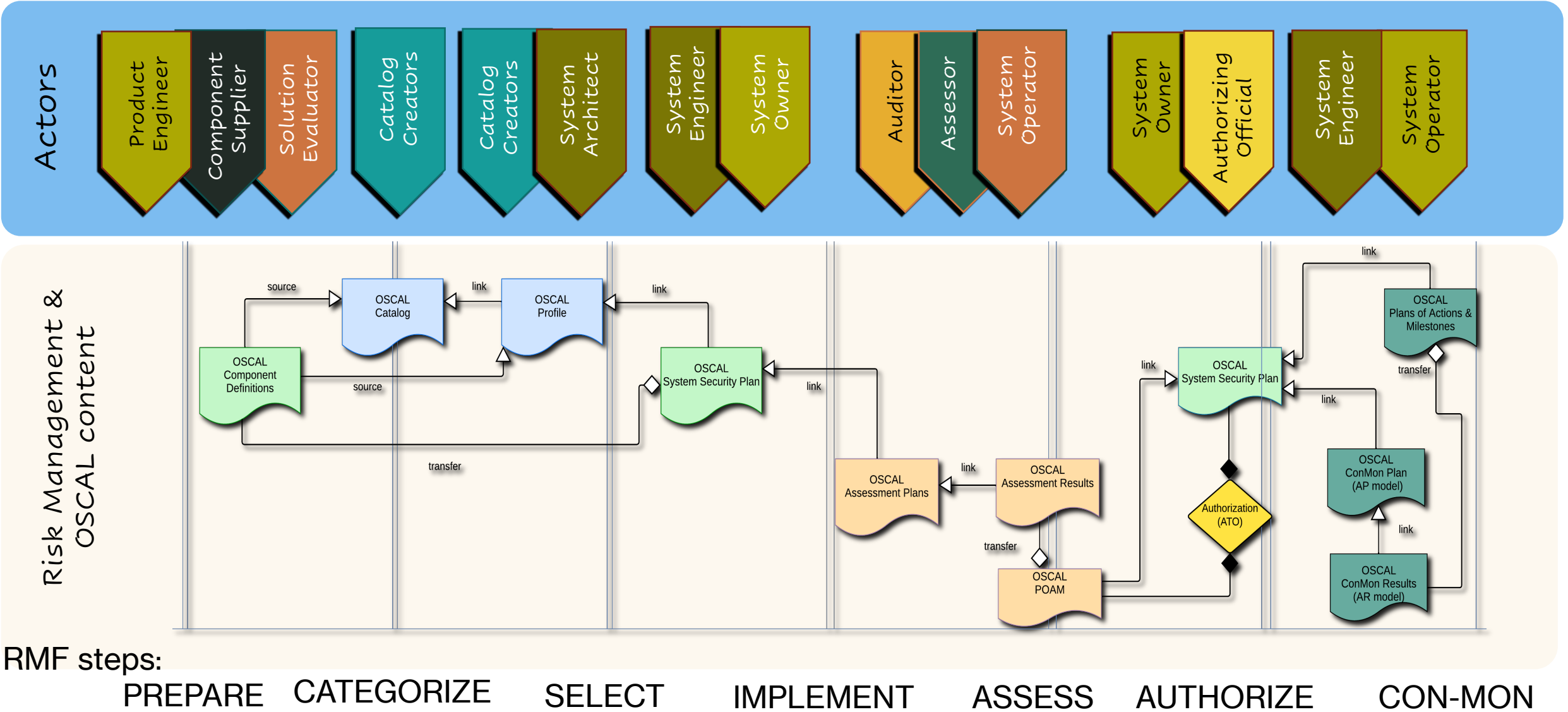


Risk Management with OSCAL



- ❑ Any requirement, policy or control can be digitalized for machines (GRC tools) to consume.
 - designed for security, demonstrated applicability to privacy, safety, usability, identity management requirements, etc.
- ❑ Information-driven process.

OSCAL Models & RMF



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 & Reference

OSCAL

About Learn Concepts **Reference** Downloads Tools Contribute

Model Reference

Data Types

Release Notes

Development Snapshot

Latest Release (v1.0.4)

All Models

JSON Outline

JSON Reference

JSON Index

JSON Metaschema Reference

XML Outline

XML Reference

XML Index

XML Metaschema Reference

Assessment Plan Model

Assessment Results Model

Catalog Model

Component Definition Model

Plan of Action and Milestones Model

Complete v1.1.3 XML Format Outline

The following outline is a representation of the [XML Format Reference](#) for the combination of all OSCAL models. For each element corresponding entry in the [XML Format Reference](#). The cardinality and data type are also provided for each element of

```
<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
  <metadata> ...
  <import-comp
  <component u
  <capability
  <back-matter
</component-defini
  <system-security
  <assessment-plan
  <assessment-resu
  <plan-of-action-
```

OSCAL

About Learn Concepts **Reference** Downloads Tools Contribute

Model Reference

Data Types

Release Notes

Development Snapshot

Latest Release (v1.0.4)

All Models

JSON Outline

JSON Reference

JSON Index

JSON Metaschema Reference

XML Outline

XML Reference

XML Index

XML Metaschema Reference

Assessment Plan Model

Assessment Results Model

Catalog Model

Component Definition Model

Plan of Action and Milestones Model

Complete v1.0.4 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 element or attribute. 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
  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-values:
    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.
    - source-profile: The tool used to produce a resolved profile.
  value:
    The value must be one of the following:
    - resolution-tool: The tool used to produce a resolved profile.
    - source-profile: The tool used to produce a resolved profile.
  properties: (6)
  uuid: uuid [1]
    description: A globally unique identifier with cross-instance scope for this catalog instance. This UUID should be changed when this document is revised.
  metadata: metadata [1]
    description: A globally unique identifier with cross-instance scope for this catalog instance. This UUID should be changed when this document is revised.
```

OSCAL

About Learn Concepts **Reference** Downloads Tools Contribute

Model Reference

Data Types

Release Notes

Development Snapshot

Latest Release (v1.0.4)

All Models

JSON Outline

JSON Reference

JSON Index

JSON Metaschema Reference

XML Outline

XML Reference

XML Index

XML Metaschema Reference

Assessment Plan Model

Assessment Results Model

Catalog Model

Component Definition Model

Plan of Action and Milestones Model

Complete v1.1.3 JSON Format Outline

The following outline is a representation of the [JSON Format Reference](#) 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 [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
  uuid [1]
  <metadata
  <import-comp
  <component u
  <capability
  <back-matter
</component-defini
  <system-security
  <assessment-plan
  <assessment-resu
  <plan-of-action-
```

OSCAL

About Learn Concepts **Reference** Downloads Tools Contribute

Model Reference

Data Types

Release Notes

Development Snapshot

Latest Release (v1.0.4)

All Models

JSON Outline

JSON Reference

JSON Index

JSON Metaschema Reference

XML Outline

XML Reference

XML Index

XML Metaschema Reference

Assessment Plan Model

Assessment Results Model

Catalog Model

Component Definition Model

Plan of Action and Milestones Model

Complete v1.0.4 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
  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-values:
    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.
    - source-profile: The tool used to produce a resolved profile.
  value:
    The value must be one of the following:
    - resolution-tool: The tool used to produce a resolved profile.
    - source-profile: The tool used to produce a resolved profile.
  properties: (6)
  uuid: uuid [1]
    description: A globally unique identifier with cross-instance scope for this catalog instance. This UUID should be changed when this document is revised.
  metadata: metadata [1]
    description: A globally unique identifier with cross-instance scope for this catalog instance. This UUID should be changed when this document is revised.
```


https://github.com/usnistgov/OSCAL

```
▼ 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]: {
```

OSCAL Models/Schemas

```
▶ metadata [1]: { _ },
▶ import-profile [1]: { _ },
▶ system-characteristics [1]: { _ },
▶ system-implementation [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-ap [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]: { _ },
}
```

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

usnistgov / oscal-content Public

<> Code Issues 22 Pull requests 2

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

draft

NIST_SP-800-53_rev5_PRIVACY-baseline_profile...

NIST_SP-800-53_rev5_PRIVACY-baseline_profile.xml

NIST_SP-800-53_rev5_PRIVACY-baseline_profile.xml

NIST_SP-800-53_rev5_catalog.xml

OSCAL Content (Artifacts)

OSCAL Content Operationalized

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

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
		A library of reusable ReaT	

OSCAL Editorial Tools

		systems might manipulate catalogs, profiles, components, and SSPs.	source
XSLT Tooling	NIST OSCAL Project	A variety of Extensible Stylesheet Language (XSL) Transformations (XSLT), 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 is a cyber risk management and compliance analytics platform that enables users	

OSCAL GRC Tools

Compliance Automation	C2 Labs	for catalogs, policies, 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 Catalog Model

Catalog Tutorial: <https://pages.nist.gov/OSCAL/tutorials/catalog/catalog-sample/>

A `<catalog>` contains:

- `<metadata>` (required) - Provides document metadata for the catalog.
- `<group>` (optional) - Allows for grouping of `<control>` and other `<group>` elements. Zero or more `<group>` elements may be used.
- `<control>` (optional) - Defines a given control in the catalog. Zero or more `<control>` elements may be used, and a `<control>` can be nested within another `<control>` element to identify an optional portion of a control that can be managed as a discrete unit (e.g., a control enhancement).
- `<back-matter>` (optional) – Contains references used within the catalog.

EXAMPLE: A 27002 CONTROL (PROSE)

1.1.2 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 (XML):

1.1.2 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.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <?xml-model schematypens="http://www.w3.org/2001/XMLSchema" type="application/xml" href="https://github.com/usnistgov/OSCA
3 <catalog xmlns="http://csrc.nist.gov/ns/oscal/1.0"
4   uuid="74c8ba1e-5cd4-4ad1-bbfd-d888e2f6c724">
5   <metadata>
6     <title>Sample Security Catalog <em>for Demonstration</em> and Testing</title>
7     <published>2023-10-12T00:00:00.000000-04:00</published>
8     <last-modified>2025-08-26T17:57:28.355446-04:00</last-modified>
9     <version>1.1</version>
10    <oscal-version>1.1.3</oscal-version>
11    <remarks>
12      <p>The following is a short excerpt from <a href="https://www.iso.org/standard/54533.html">ISO/IEC 27002:2013</a>
13    </remarks>
14  </metadata>
15  <group id="s1">
16    <title>Organization of Information Security</title>
17    <prop name="label" value="1"/>
18    <group id="s1.1">
19      <title>Internal Organization</title>
20      <control id="s1.1.1" >...
64    </control>
65    <control id="s1.1.2">
66      <title>Segregation of duties</title>
67      <prop name="label" value="1.1.2"/>
68      <part id="s1.1.2_stm" name="statement">
69        <p>Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthor
70      </part>
71      <part id="s1.1.2_gdn" name="guidance">
72        <part id="s1.1.2_gdn.1" name="assessment-objective">
73          <p>Care should be taken that no single person can access, modify or use assets without authorization or
74        </part>
75        <part id="s1.1.2_gdn.2" name="assessment-objective">
76          <p>Small organizations may find segregation of duties difficult to achieve, but the principle should be
77        </part>
78      </part>
79      <part id="s1.1.2_inf" name="overview">
80        <p>Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organiz
81      </part>
82    </control>
83  </group>
84 </group>
```

EXAMPLE (JSON & YAML - snippets):

```
{
  "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."
  } ]
}
```

```
- 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.
```


Traceability Example (Profile)

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <profile xmlns="http://csrc.nist.gov/ns/oscal/1.0"
3   uuid="c0dc468c-934e-4fe9-b5bf-9fc63f5a2915">
4   <metadata>
5     <title>Sample Security Profile <em>For Demonstration</em> and Testing
6   </title>
7     <last-modified>2025-08-26T10:31:28.355446-04:00</last-modified>
8     <version>1.0</version>
9     <oscal-version>1.1.3</oscal-version>
10    <remarks>
11      <p>The following document is used in the OSCAL Profile Tutorial and builds on the ca
12    </p>
13  </remarks>
14  </metadata>
15  <import href="../../catalog/xml/basic_catalog.xml">
16    <include-controls>
17      <matching pattern="s1.1.*"/>
18    </include-controls>
19    <include-controls>
20      <with-id>s2.1.1</with-id>
21    </include-controls>
22    <exclude-controls>
23      <with-id>s2.1.2</with-id>
24    </exclude-controls>
25  </import>
26  <merge>
27    <flat/>
28  </merge>
29  <modify>
30    <set-parameter param-id="s1.1.1-prm_2">
31      <label>a duration (maximum 30 minutes)</label>
32    </set-parameter>
33    <alter control-id="s1.1.1">
34      <add position="after" by-id="s1.1.1_gdn.3">
35        <part id="s1.1.1_gdn.4" name="assessment-objective" class="assessment-objective">
36          <p>Users of devices running Gnome can adjust the inactivity timeout using the fo
37        </p>
38      </add>
39    </alter>
40  </modify>
41 </profile>
```

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <catalog xmlns="http://csrc.nist.gov/ns/oscal/1.0"
3   uuid="603fb519-5ac1-48ca-9612-8174faa0354a">
4   <metadata> ...
5 </metadata>
6   <control id="s1.1.1">
7     <title>Information security roles and responsibilities</title>
8     <param id="s1.1.1-prm1">
9       <label>a choice from a selection</label>
10      <select how-many="one-or-more">
11        <choice>initiating a device lock after <insert type="param" id-ref="s1.1.1-prm_2"/> of
12        <choice>requiring the user to initiate a device lock before leaving the system unattend
13      </select>
14    </param>
15    <param id="s1.1.1-prm_2">
16      <label>a duration (maximum 30 minutes)</label>
17    </param>
18    <prop name="label" value="1.1.1"/>
19    <part id="s1.1.1_smt" name="overview">
20      <p>To establish a management framework to initiate and control the implementation and oper
21    </p>
22    </part>
23    <part id="s1.1.1_stm" name="statement">
24      <p>All information security responsibilities should be defined and allocated.</p>
25      <p>A value has been assigned to <insert type="param" id-ref="s1.1.1-prm1"/>.</p>
26      <p>A cross link has been established with a choppy syntax: <a href="#s1.1.2">(choppy)</a>.</p>
27    </part>
28    <part id="s1.1.1_gdn" name="guidance">
29      <part id="s1.1.1_gdn.1" name="assessment-objective">
30        <p>Allocation of information security responsibilities should be done in accordance wit
31      </p>
32    </part>
33    <part id="s1.1.1_gdn.2" name="assessment-objective">
34      <p>Individuals with allocated information security responsibilities may delegate securi
35    </p>
36    </part>
37    <part id="s1.1.1_gdn.3" name="assessment-objective"> ...
38  </part>
39    <part id="s1.1.1_gdn.4"
40      name="assessment-objective"
41      class="assessment-objective">
42      <p>Users of devices running Gnome can adjust the inactivity timeout using the following
43    </p>
44  </part>
45  <part id="s1.1.1_inf" name="overview"> ...
46 </part>
47 </control>
48 <control id="s1.1.2"> ...
49 </control>
50 <control id="s2.1.1"> ...
51 </control>
52 </catalog>
```

Control Mapping Model v1.2.1 JSON Format Outline

The following outline is a representation of the JSON format for this [model](#), whose schema can be found [here](#). 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.

```
mapping-collection [1]: {
  uuid [1]: uuid,
  ▶ metadata [1]: { ... },
  ▶ provenance [1]: { ... },
  ▼ mappings [1]: [
    Array members, or a singleton mapping object [1 to ∞] {
      uuid [1]: uuid,
      method [0 or 1]: string,
      matching-rationale [0 or 1]: string,
      status [0 or 1]: string,
      ▶ source-resource [1]: { ... },
      ▶ target-resource [1]: { ... },
      ▼ maps [1]: [
        An array of map objects [1 to ∞] {
          uuid [1]: uuid,
          ns [0 or 1]: uri,
          matching-rationale [0 or 1]: string,
          relationship [1]: token,
          ▶ sources [1]: [ ... ],
          ▶ targets [1]: [ ... ],
          ▶ qualifiers [0 or 1]: [ ... ],
          ▶ confidence-score [0 or 1]: { ... },
          ▶ coverage [0 or 1]: { ... },
          ▶ props [0 or 1]: [ ... ],
          ▶ links [0 or 1]: [ ... ],
          remarks [0 or 1]: markup-multiline
        },
        ▶ props [0 or 1]: [ ... ],
        ▶ links [0 or 1]: [ ... ],
        remarks [0 or 1]: markup-multiline,
        mapping-description [0 or 1]: markup-multiline,
        ▶ source-gap-summary [0 or 1]: { ... },
        ▶ target-gap-summary [0 or 1]: { ... },
        ▶ confidence-score [0 or 1]: { ... },
        ▶ coverage [0 or 1]: { ... }
      ],
      ▶ back-matter [0 or 1]: { ... },
    }
  ]
}
```

matching-rationalestring[0 or 1]Switch to XML

Matching

DESCRIPTIONThe method used for relating controls within the mapping. The supported methods are aligned with the [NIST Interagency Report \(IR\) 8477](#), Section 4.3 Set Theory Relationship Mapping.

▼ Remarks

The value of this flag applies to the entire document if found in the top-level mapping provenance, otherwise it applies to the specific mapping in which it is found.

If this flag appears in both locations, the lower-scoped value overrides while within it's scope.

▼ Constraint (1)

ALLOWED VALUES

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

- **syntactic**: Syntactic: How similar is the wording that expresses the two concepts. This is a word-for-word analysis of the relationship, not an interpretation of the language.
- **semantic**: Semantic: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
- **functional**: Functional: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.



relationshiptoken[1]Switch to XML

Mapping Entry Relationship

DESCRIPTIONThe relationship type for the mapping entry, which describes the relationship between the effective requirements of the specified source and target sets in the context of the [matching-rationale](#) method globally defined in the [provenance](#) unless overwritten locally in the [map](#). The [relationship](#) type and the [matching-rationale](#) must be used together. However, more than one [matching-rationale](#) method may apply to a [source](#) and [target](#) pair.

▼ Remarks

For example, consider the CSF 1.1's PR.AC-1, "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes", and the Privacy Framework's PR.AC-P1, "Identities and credentials are issued, managed, verified, and devices."

These two requirements have identical wording except for "users" versus "individuals" and the order of the last few words. With a `matching-rationale` of syntactic, the relationship type would beintersects with because the two overlap, but each includes content that the other does not. However, with a rationale of semantic, the relationship type would be equal if "users" and "individuals" have the same meaning in their respective sources, subset if "users" was a subset of "individuals," and so on.

When establishing relationships, mapping SHOULD be done at the control statement level where possible. This approach allows for a more accurate relationship.

▼ Constraint (1)

ALLOWED VALUESfor `[.has-oscal-namespace('http://csrc.nist.gov/ns/oscal')]`

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

- **equivalent-to**: The source and target requirements are similar, although not necessarily identical. The words may differ, but both mapped sets convey similar information with the same effective meaning. This relationship may be reversed, since `A equivalent-to B` also means that `B equivalent-to A`. This relationship is less suitable for a syntactic matching-rationale.
- **equal-to**: The source and target requirements are the same. Differences in capitalization, spelling, and grammar can be ignored, if these differences do not change the meaning. This relationship may be reversed, since `A equal-to B` also means that `B equal-to A`.
- **subset-of**: The source requirements are a subset of target requirements. In other words, target contains all source requirements and additional others. This relationship may be reversed as a `superset-of`, since `A subset-of B` also means that `B superset-of A`.
- **superset-of**: The source requirements are a superset of target requirements. In other words, source contains all target requirements and additional others. This relationship may be reversed as a `subset-of`, since `A superset-of B` also means that `B subset-of A`.
- **intersects-with**: The source and target requirements have some overlap, but each includes content that the other does not. This relationship may be reversed, since `A intersects-with B` also means that `B intersects-with A`. A mapping at statement level could result on relationships mapping that allows for more inference than using this relationship type.
- **no-relationship**: The source and target requirements are not related; their content does not overlap. This relation is introduced not with the intention to support exhaustiv mapping of all requirements and statements that have no overlap, but rather to support edge cases such is the need to tailor a relationship in the context of a component or system to better align with the implementation and configuration of the respective component or system. Also, this relationship is provided in support of the NIST IR 8477.

mapping-collection

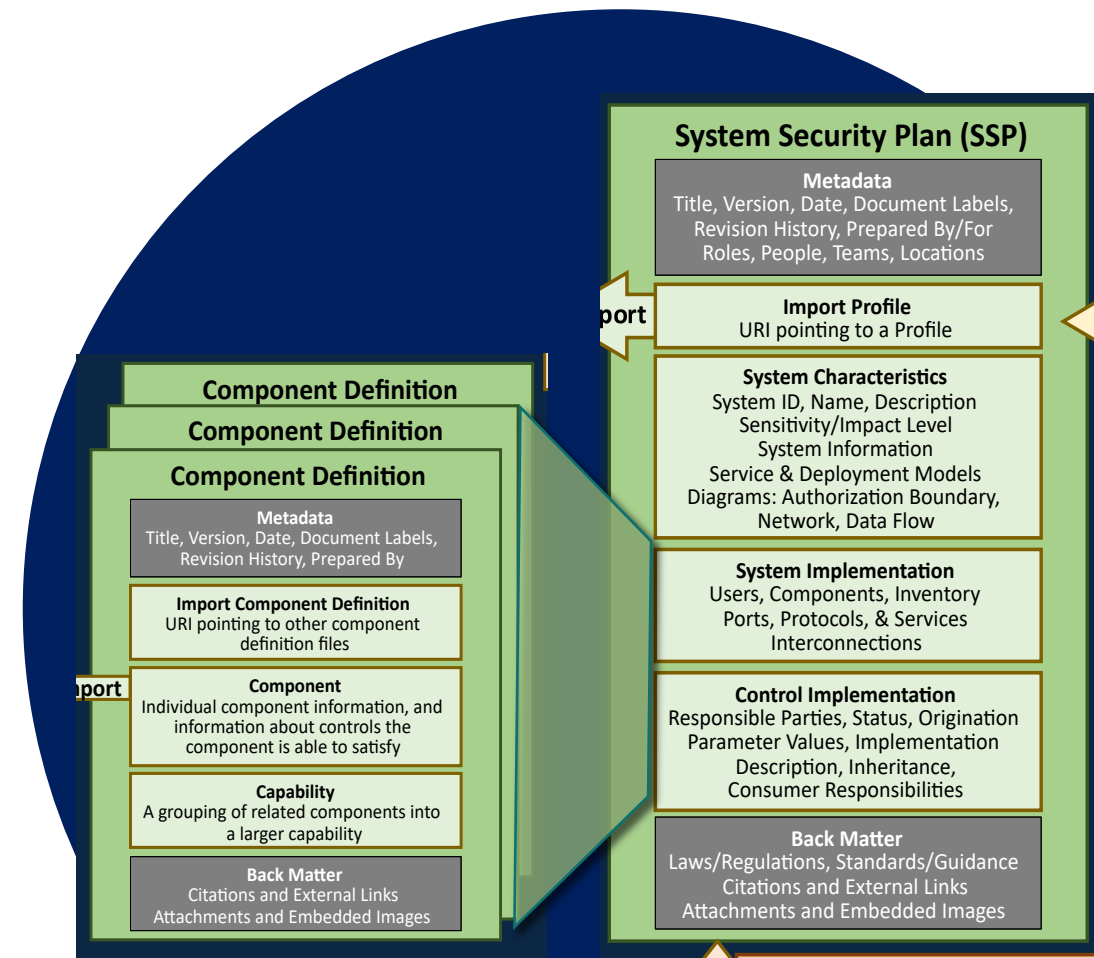
- uuid
- metadata
- provenance
- mappings
 - uuid
 - method
 - matching-rationale
 - status
 - source-resource
 - target-resource
 - maps
 - uuid
 - ns
 - matching-rationale
 - relationship**
 - sources
 - targets
 - qualifiers
 - confidence-score
 - coverage
 - props
 - links
 - remarks
 - props
 - links
 - remarks
 - mapping-description
 - source-gap-summary
 - target-gap-summary

- back-matter

Shifting Left with OSCAL

Implementation Layer

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



Cybersecurity 'Shipping Container*'

OSCAL artifacts are like the maritime shipping containers!

EXAMPLE: 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 Component Definition ...

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

Component Definition Model v1.1.3 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.

```
▼ 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 & Implemented Requirements

<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,  
      }  
    ],  
  }  
],  
{  
  ],  
}
```

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

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

Snippet of a Component Definition Instance in JSON

<https://github.com/usnistgov/oscal-content/blob/main/examples/component-definition/json/example-component-definition.json>

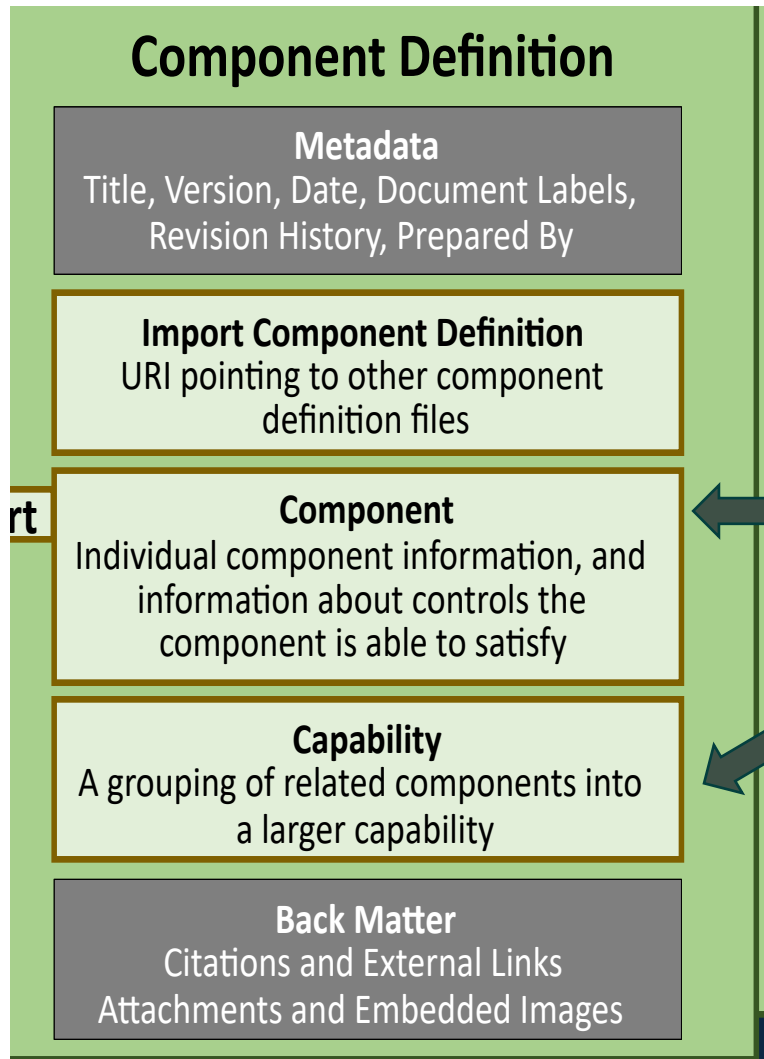
NOTE: some OSCAL assemblies
(e.g. `responsible-roles`,
`protocols`, etc.) are collapsed

```
{
  "component-definition": {
    "uuid": "a7ba800c-a432-44cd-9075-0862cd66da6b",
    "metadata": { ... },
    "components": [
      {
        "uuid": "91f646c5-b1b6-4786-9ec3-2305a044e217",
        "type": "software",
        "title": "MongoDB",
        "description": "MongoDB is a source-available, cross-platform document-oriented database program.",
        "purpose": "Provides a NoSQL database service",
        "responsible-roles": [ ... ],
        "protocols": [ ... ],
        "control-implementations": [
          {
            "uuid": "49f0b690-ed9f-4f32-aae0-625b77aa6d27",
            "source": "https://github.com/usnistgov/oscal-content/blob/master/nist.gov/SP800-53/rev5/xml/...",
            "description": "MongoDB control implementations for NIST SP 800-53 revision 5.",
            "implemented-requirements": [
              {
                "uuid": "cf8338c5-fb6e-4593-a4a8-b3c4946ee2a0",
                "control-id": "sc-8.1",
                "description": "MongoDB supports TLS 1.x to encrypt data in transit, preventing unauthorized access to sensitive information."
              },
              {
                "uuid": "cf8338c5-fb6e-4593-a4a8-b3c4946ee2a0",
                "control-id": "sa-4.9",
                "description": "Must ensure that MongoDB only listens for network connections on authorized ports."
              }
            ]
          }
        ]
      }
    ]
  }
}
```

OSCAL & SBOMs are Complementary

Data Type	SPDX	CycloneDX	OSCAL
Software component metadata	✓	✓	✓ (indirectly)
Licenses and legal info	✓	✓	✗
Package relationships (dependencies)	✓	✓	✓ (modelable)
Vulnerability info	Limited	✓	✓
Security controls	✗	Limited	✓
Provenance & trust (e.g., hashes)	✓	✓	✓
Cryptographic elements (signatures)	✓ (optional)	✓	✓

Component Definitions & BOMs



Link to a SWID

Import Component Defs

Link to component's (S)BOM or (H)BOM depending on its type. (SPDX, CyclonDX)

```
component-definition [1]: {
  uuid [1]: uuid,
  metadata [1]: {
    title [1]: markup-line,
    published [0 or 1]: date-time-with-timezone,
    last-modified [1]: date-time-with-timezone,
    version [1]: string,
    oscal-version [1]: string,
    revisions [0 or 1]: [ - ],
    document-ids [0 or 1]: [ - ],
    props [0 or 1]: [ - ],
    links [0 or 1]: [ - ],
    roles [0 or 1]: [ - ],
    locations [0 or 1]: [ - ],
    parties [0 or 1]: [ - ],
    responsible-parties [0 or 1]: [ - ],
    actions [0 or 1]: [ - ],
    remarks [0 or 1]: markup-multiline,
  },
  import-component-definitions [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]: [ - ],
      responsible-roles [0 or 1]: [ - ],
      protocols [0 or 1]: [ - ],
      control-implementations [0 or 1]: [ - ],
      remarks [0 or 1]: markup-multiline,
    }
  ],
  capabilities [0 or 1]: [
    An array of capability objects [1 to ∞] {
      uuid [1]: uuid,
      name [1]: string,
      description [1]: markup-multiline,
      props [0 or 1]: [ - ],
      links [0 or 1]: [ - ],
      incorporates-components [0 or 1]: [ - ],
      control-implementations [0 or 1]: [ - ],
      remarks [0 or 1]: markup-multiline,
    }
  ],
  back-matter [0 or 1]: { - },
}
```

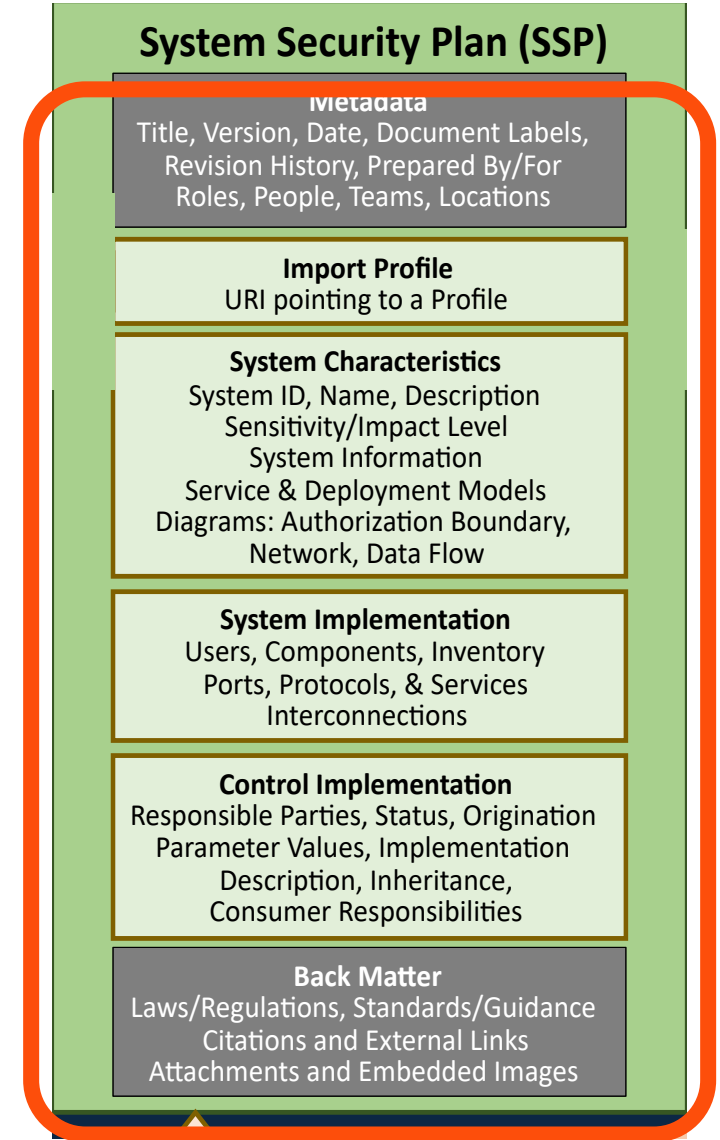

The SSP Model

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

System Security Plan Model 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.

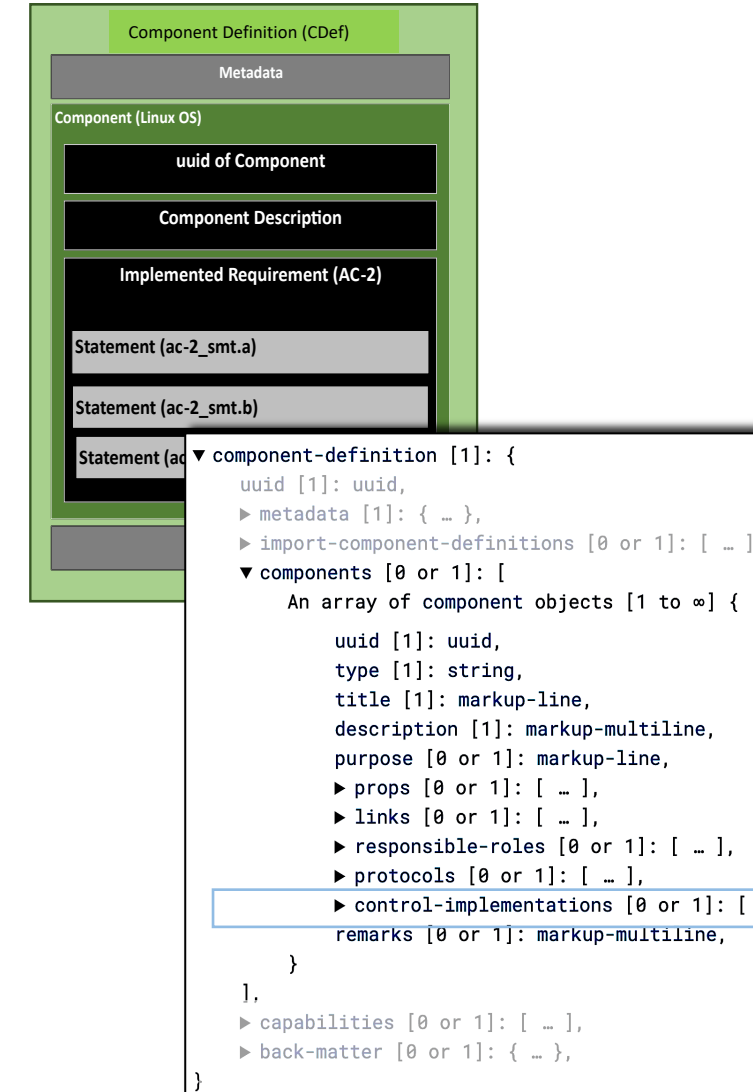
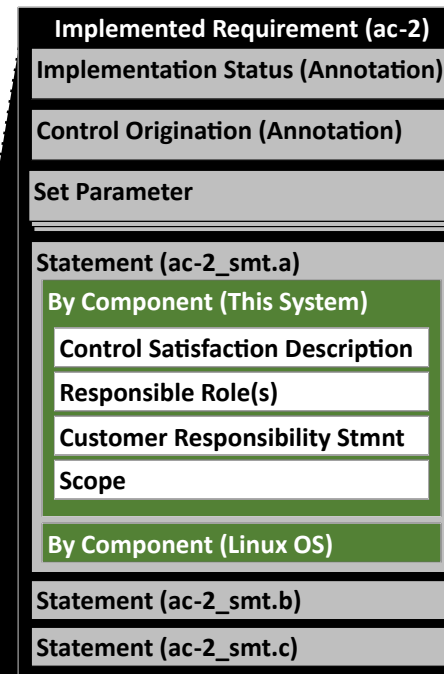
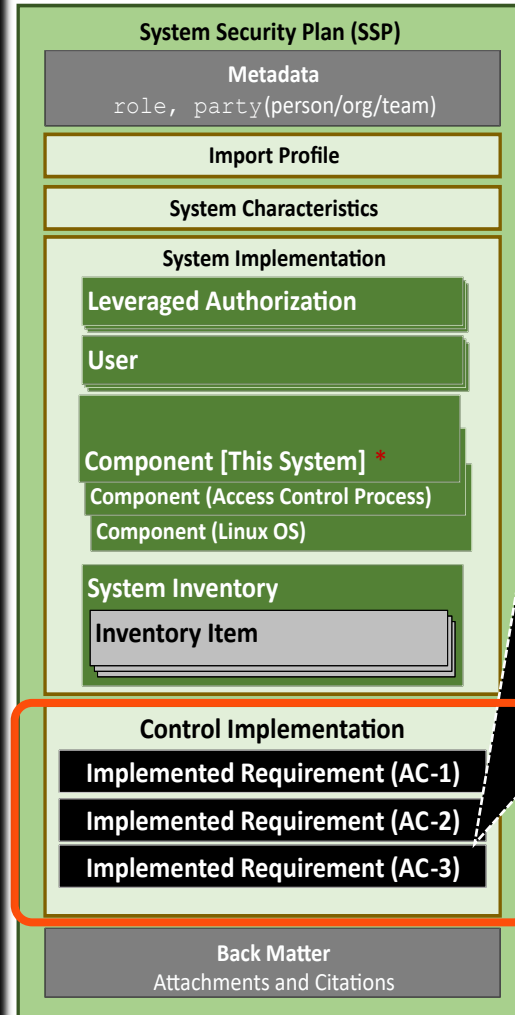
```
▼ system-security-plan [1]: {  
  uuid [1]: uuid,  
  ► metadata [1]: { ... },  
  ► import-profile [1]: { ... },  
  ► system-characteristics [1]: { ... },  
  ► system-implementation [1]: { ... },  
  ► control-implementation [1]: { ... },  
  ► back-matter [0 or 1]: { ... }  
}
```



The System Security Plan Model ...

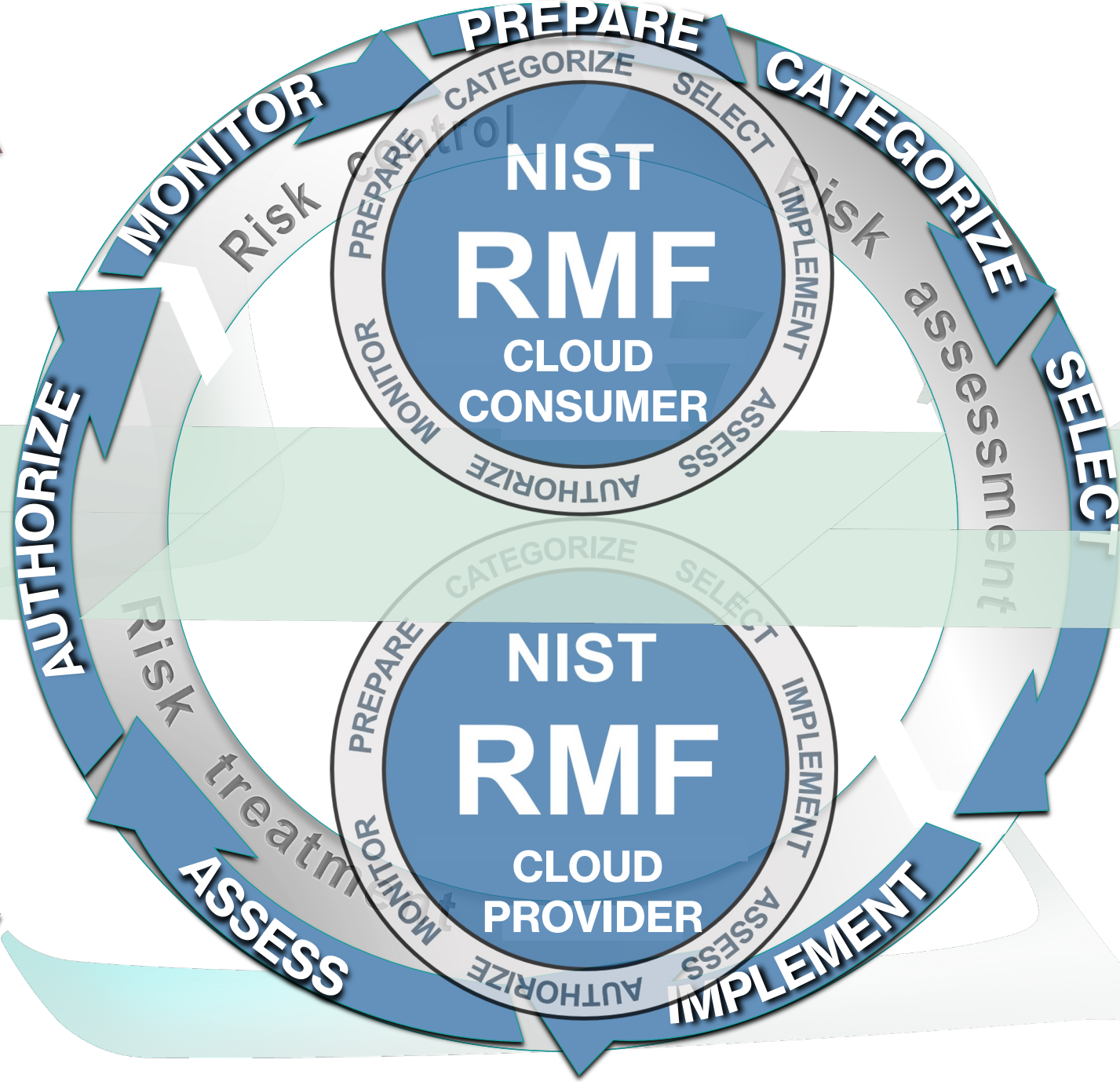
<https://pages.nist.gov/OSCAL/reference/latest/system-security-plan/json-outline/>

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

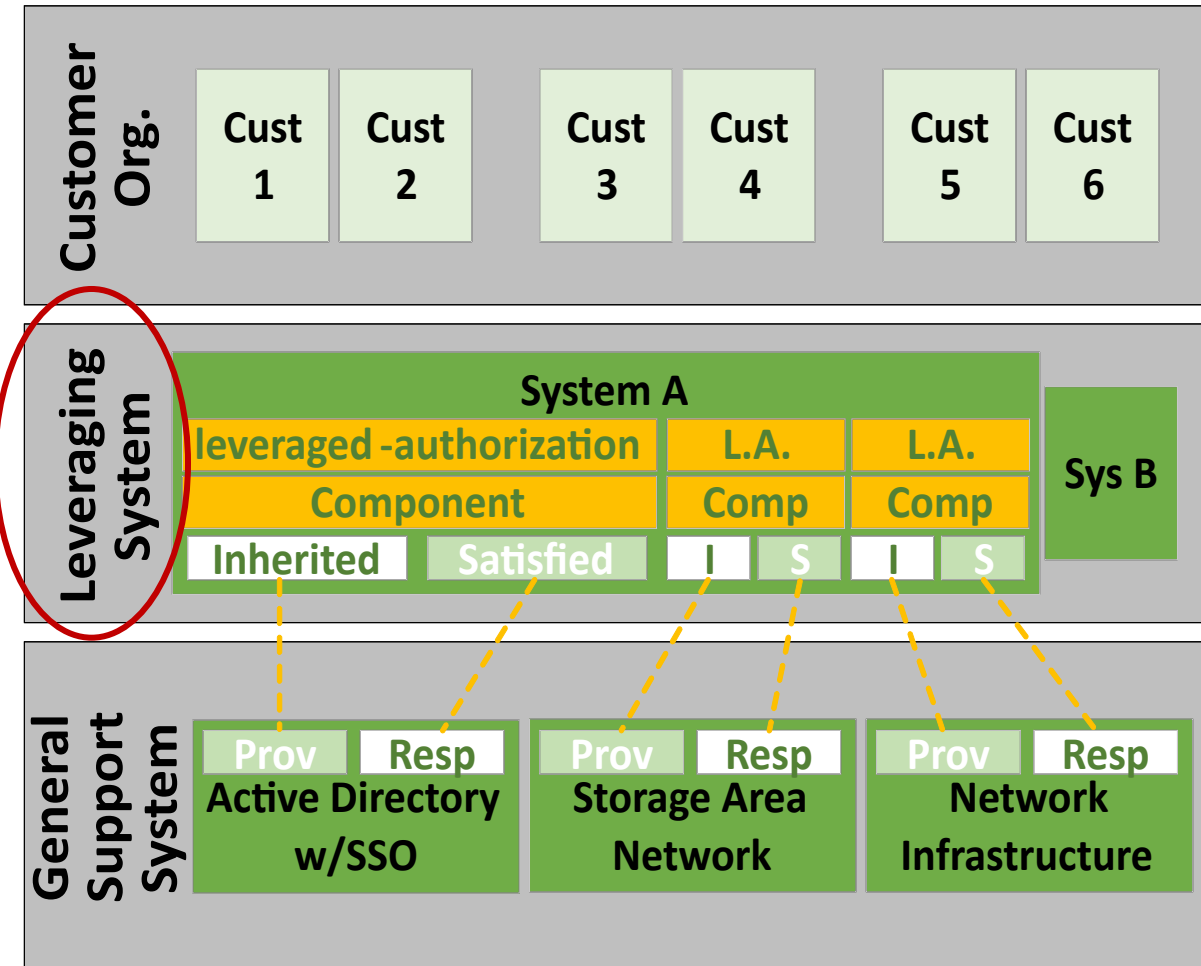
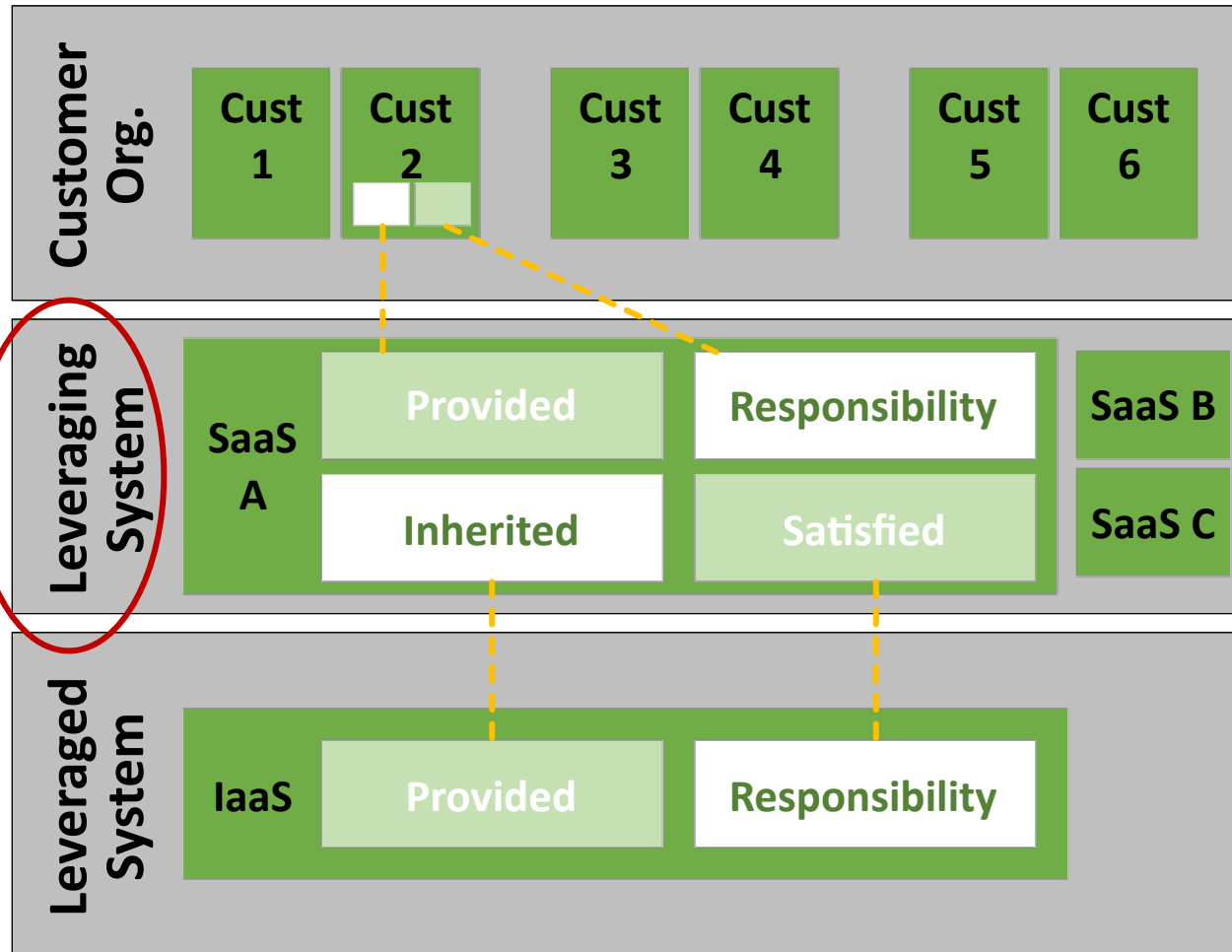


**Layers Managed
by Providers**

**Layers Managed
by Consumers**



The Shared Responsibility (SR) Model (prototype)

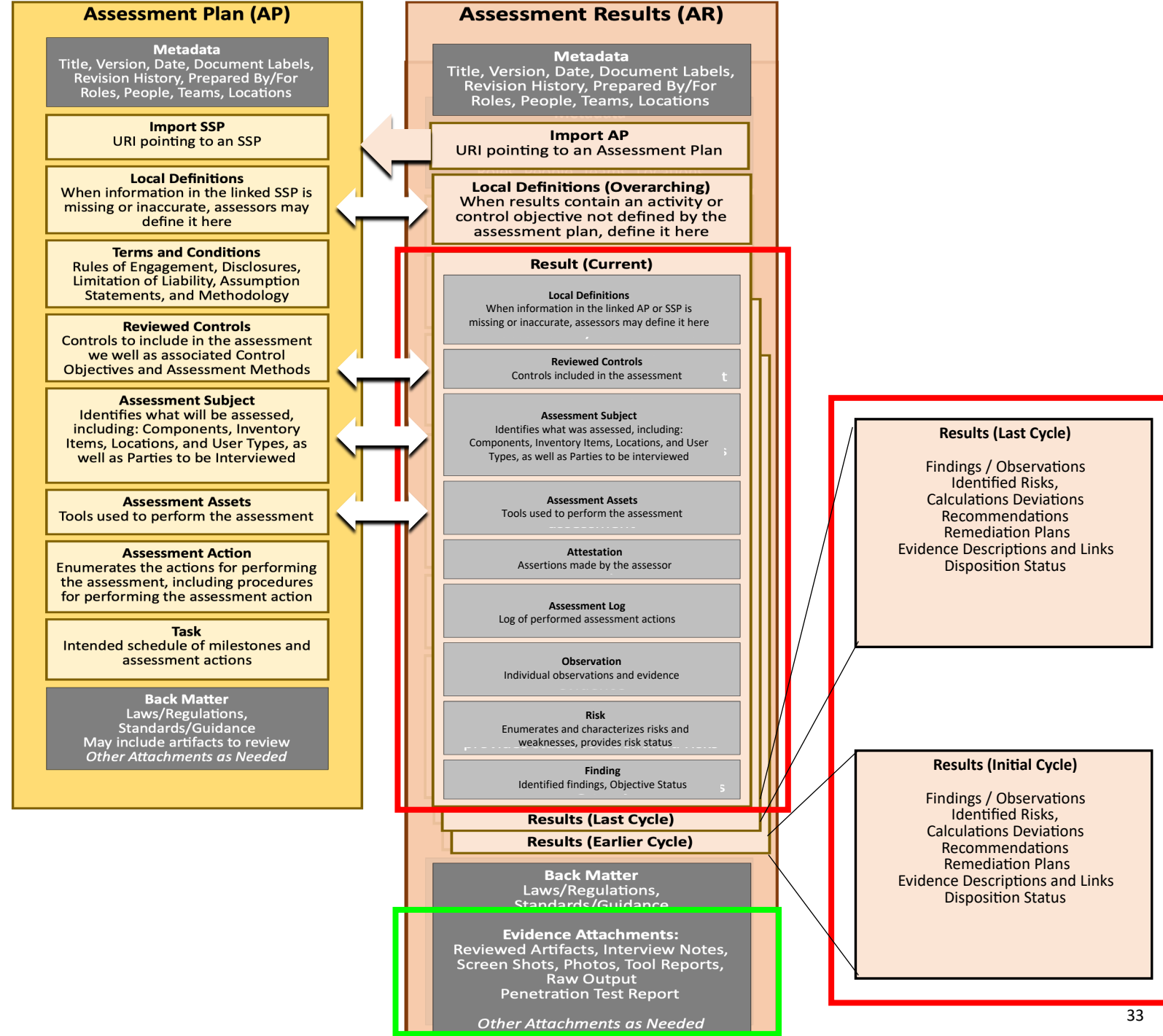


Assessment Plan (AP) & Assessment Results (AR)

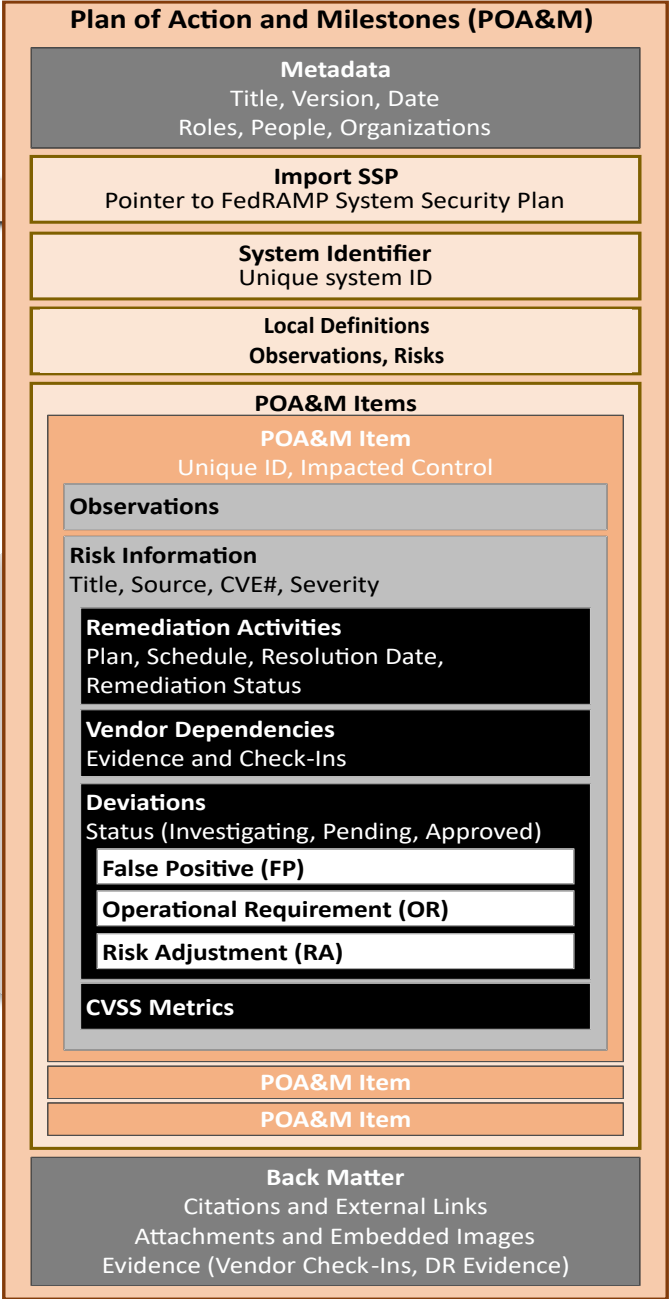
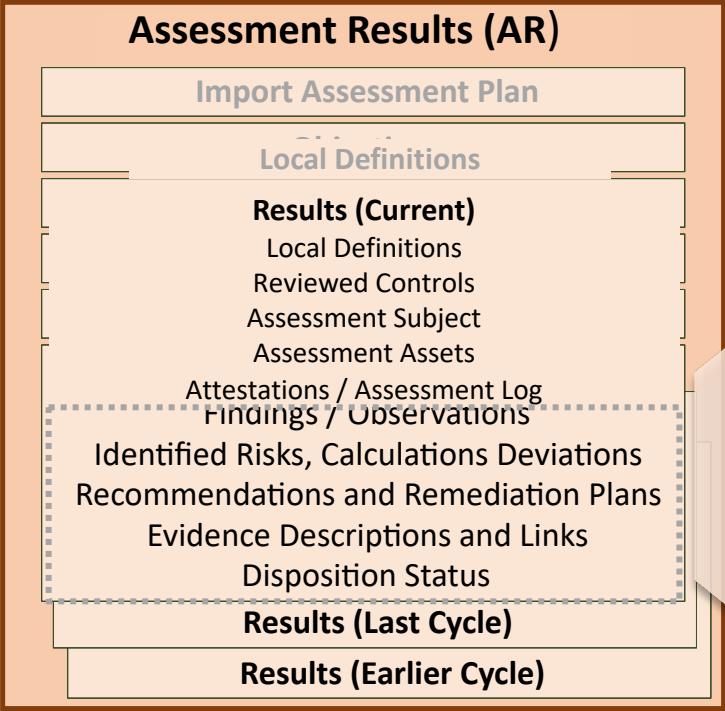
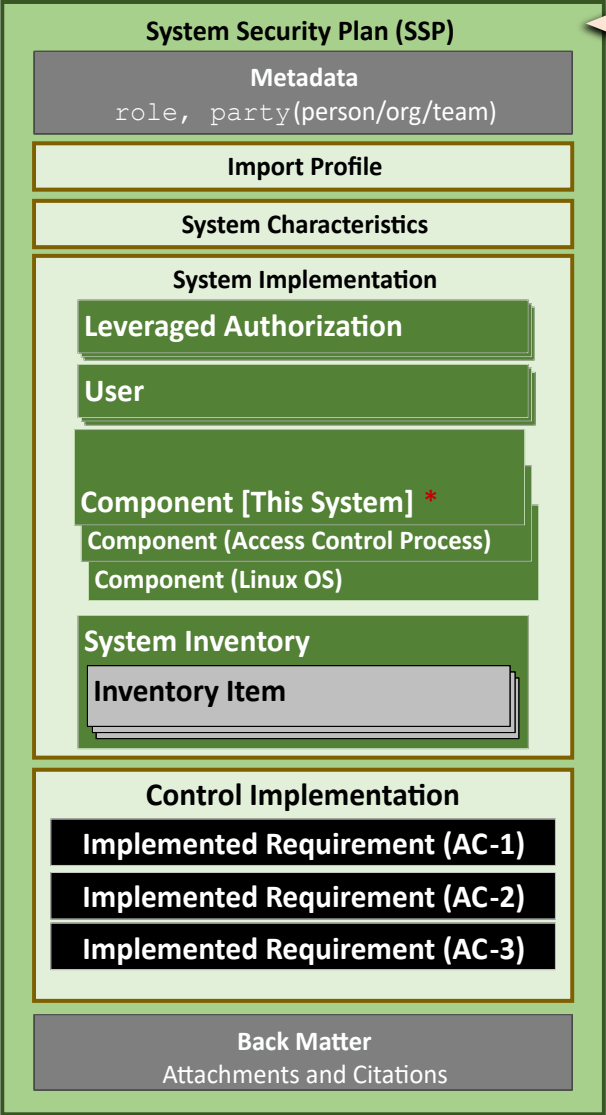
- ❑ Overlapping syntax
- ❑ Similar but distinct purposes
- ❑ Unique to AR: Results and Evidence

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



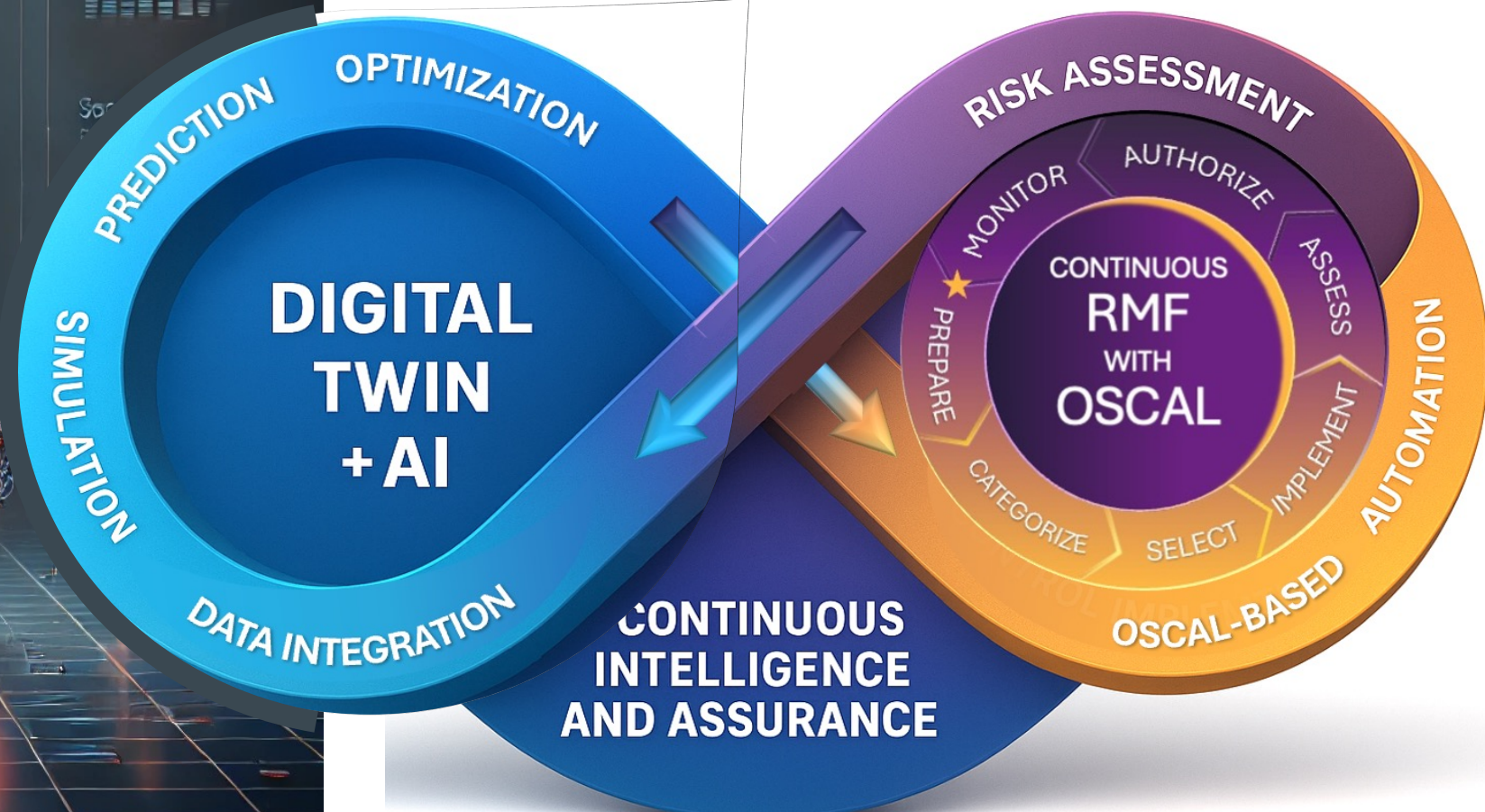
Sometimes Security Is Not Enough – Resilience Is the Key



OSCAL supports:

- ☐ Security left-shifting by pre-assessing the system's components
- ☐ Include pointers to SBOMs (when applicable)
- ☐ Assessment of only component's deployments specifics.
- ☐ Analysis of the interaction between components
- ☐ Traceability of controls to their origination and complete assessment across stacks
- ☐ Right-shifting the response to findings and identified risks

Digital Twin-based Intelligent Continuous System Risk Management



Artificial Intelligence

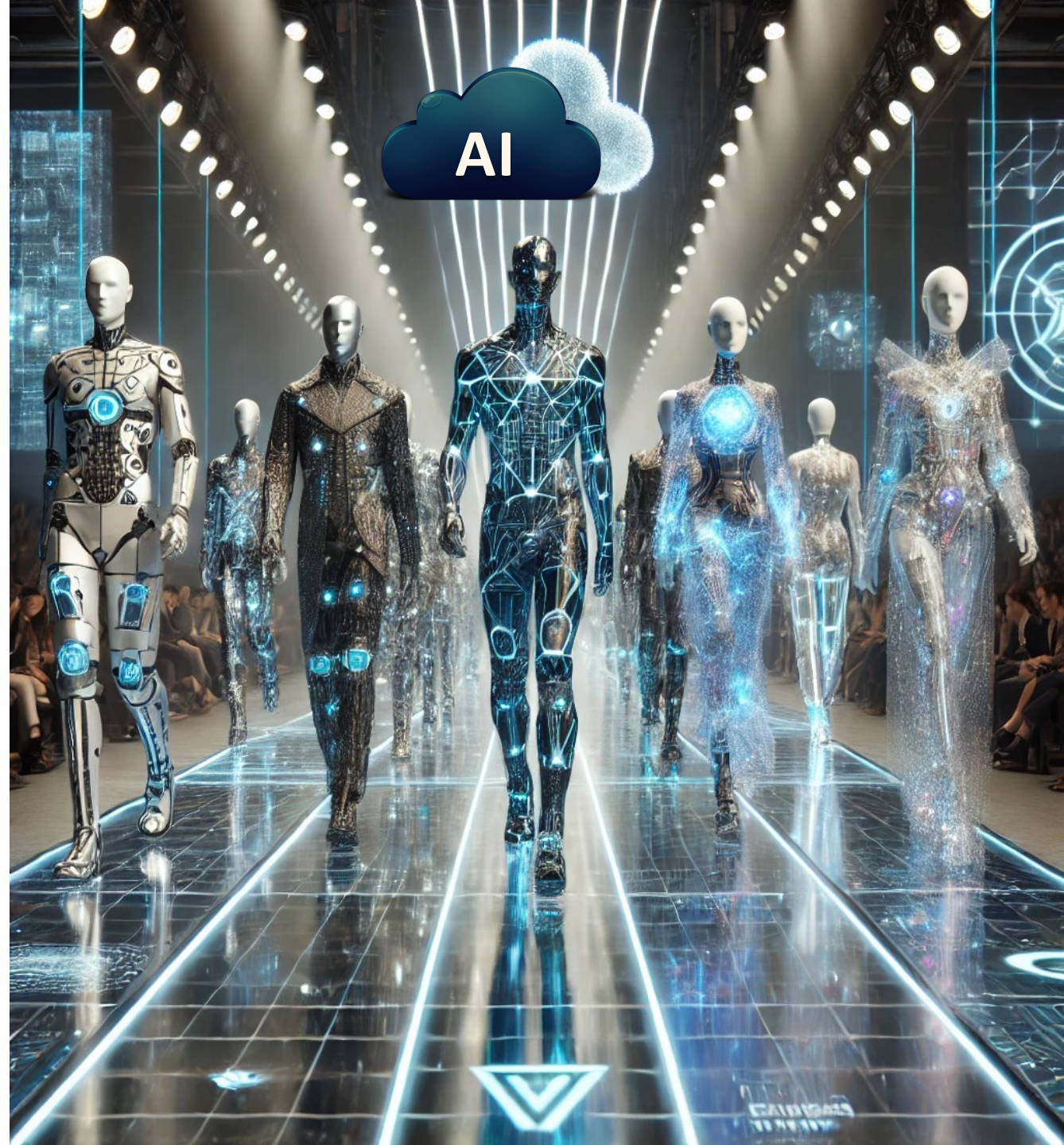
THE LATEST INFLECTION POINT IN
MODERN TECHNOLOGICAL EVOLUTION

Coupled with OSCAL formatted data, AI
eliminates extensive manual efforts by:

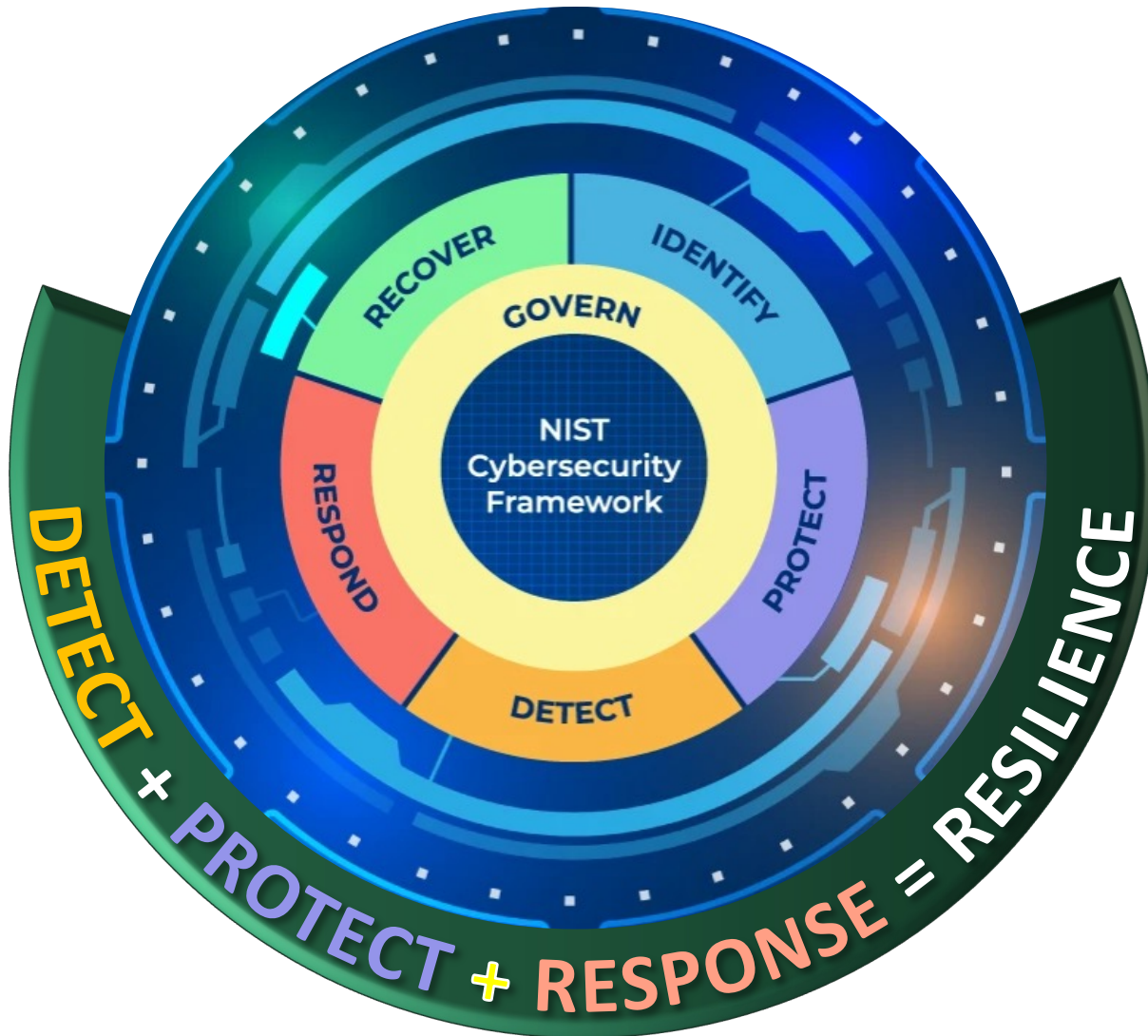
- ❑ accelerating control evaluations,
- ❑ correlating evidence,
- ❑ identifying anomalies,
- ❑ automating aspects of continuous monitoring

Essential to realizing AI full potential:

- security,
- safety,
- trustworthiness
- transparency,
- robustness,
- protection against misuse



From Cybersecurity to Resiliency



A resilient system must:

PROTECT itself by safeguarding critical services and reducing the likelihood or impact of cybersecurity events.

DETECT anomalies and threats quickly and accurately, ensuring that emerging risks are recognized before they escalate.

RESPOND promptly and effectively to detected events, containing damage and restoring normal operations

OSCAL allows those functions, their categories and subcategories as defined in the CSF, to be **digitally mapped** to controls from any adopted regulatory framework, to **continuously assess system's resilience**.

OSCAL FOUNDATION



ABOUT OSCAL FOUNDATION

The Open Security Controls Assessment Language (OSCAL) is a machine-readable language that simplifies and standardizes information system security assessments through the exchange of information via automation.

Originally developed by the National Institutes of Standards and Technology in collaboration with FedRAMP and industry, OSCAL aims to improve the efficiency, timeliness, accuracy, and consistency of

COMMUNITY INITIATIVES

OSCAL.io Goals



Community Hub

To provide community resources for OSCAL adopters and OSCAL-enabled tools



Automate Discovery

Provide an Application Programming Interface (API) for tools to automatically query for OSCAL resources



Promote Adoption

Enable new OSCAL adopters to get started

What to Expect

01

Upcoming OSCAL Events

02

OSCAL Communication

03

OSCAL Content Directory and Repository

Make your OSCAL catalogs, baselines (profiles) and component definitions available to all OSCAL tools.

04

OSCAL-Enabled Tools Directory

Find existing OSCAL-enabled tools or list your own.



The EU Friends of OSCAL

[What is OSCAL](#) [About](#) [Resources](#) [Events](#) [Blog](#)

EUROSCAL

The EU Friends of OSCAL

In order to promote the adoption of OSCAL in Europe, we are launching EUROSCAL (The EU Friends of OSCAL), as an open community of motivated individuals interested on leveraging OSCAL.

[See recent news](#)

OSCAL Club

[Our forum](#) [Our projects](#) [Help fix this site](#)

[Home](#) [Blog](#)

Define compliance objectives, realize security outcomes.

OSCAL Club is a community to discuss, test, and implement solutions at the intersection of compliance and security.

[Discuss in the forum](#)



How do you contribute?

OSCAL is a standard for saving data about an organization's security, risk management, and compliance programs in a machine-readable way.

For OSCAL to succeed, information technology executives, security professionals, security baseline authors, security assessors, and software developers must find real-world use cases, discuss what works, and discuss what needs improvement.

The Future of OSCAL

- Assess OSCAL models' maturity through international adoption
- Technology transfer - International standardization
- System telemetry collection & native integration
- Robust support for reciprocity (control mapping model)



OSCAL VIRTUAL ESCAPE ROOM

Operation: Open Sentry

Location: United States Cybersecurity & Infrastructure AI Agency (CIA2), Central Command.

Clearance: Top Secret // SCI // OSCAL PROGRAM ONLY.

The OSCALized DNA of the entire defense infrastructure is displayed in front of you.

The infrastructure's digital twin is actively updating the DNA information with all the patches and immunizations.



The silence is pierced unexpectedly by a loud alarm!

ALERT: CYBER ATTACK IN PROGRESS. OSCAL DATA TAMPERED!
Integrity Check FAILURE



The Mission: You must decode the OSCAL Problems and repair the artifacts.

Once all the artifacts are corrected, you must input the final code that will reset the process.

The workload is climbing to 99%. You **MUST HURRY!** YOU HAVE 30 MINUTES TO REVERT THE CHANGES

Key Takeaways



1

Open Security Controls Assessment Language (OSCAL) supports interoperable security automation processes with standardized, open-source digital formats.

2

OSCAL is a set of digital formats not a tool and can represent and support the regulatory frameworks of choice.

3

OSCAL + ((S/H)BOM + AI) set the foundation for building intelligent resilience and self-healing capabilities.

```
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))  
mirror_ob.select = 0  
bpy.context.selected_objects  
data.objects[one.name].select
```

```
print("please select exact  
--- OPERATOR CLASSES ---
```

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



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



MAIN Repository – there are many related ones:
<https://github.com/usnistgov/OSCAL>



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



Contact the team: oscal@nist.gov

THANK YOU !!