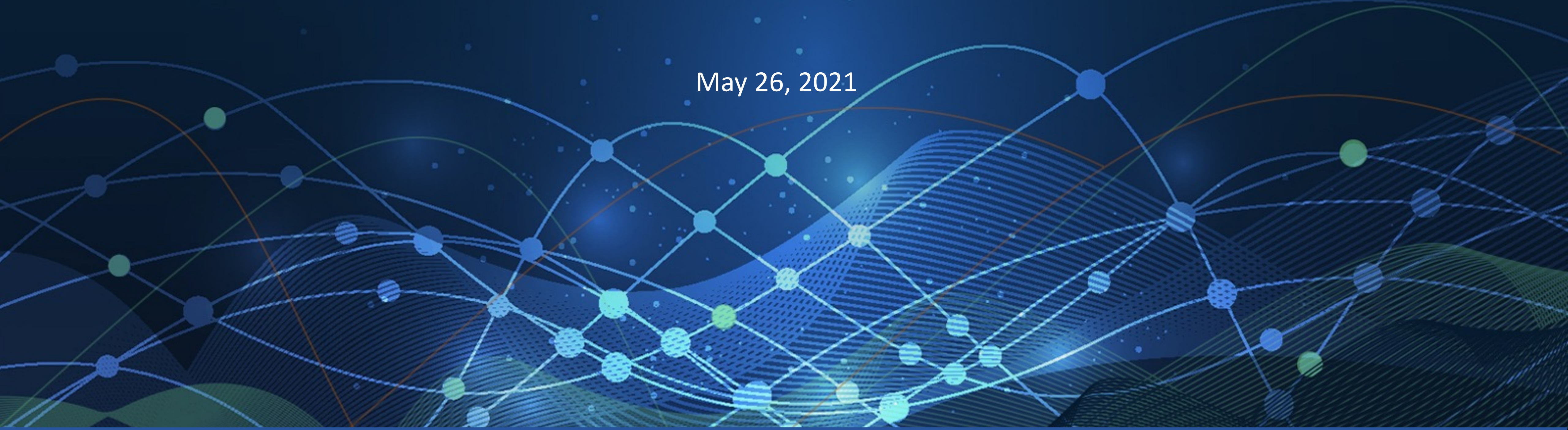
Security Automation with Open Security Controls Assessment Language (OSCAL)



May 26, 2021

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

Dr. Michaela Iorga,
OSCAL Strategic Outreach Director

Dave Waltermire,
OSCAL Technical Director

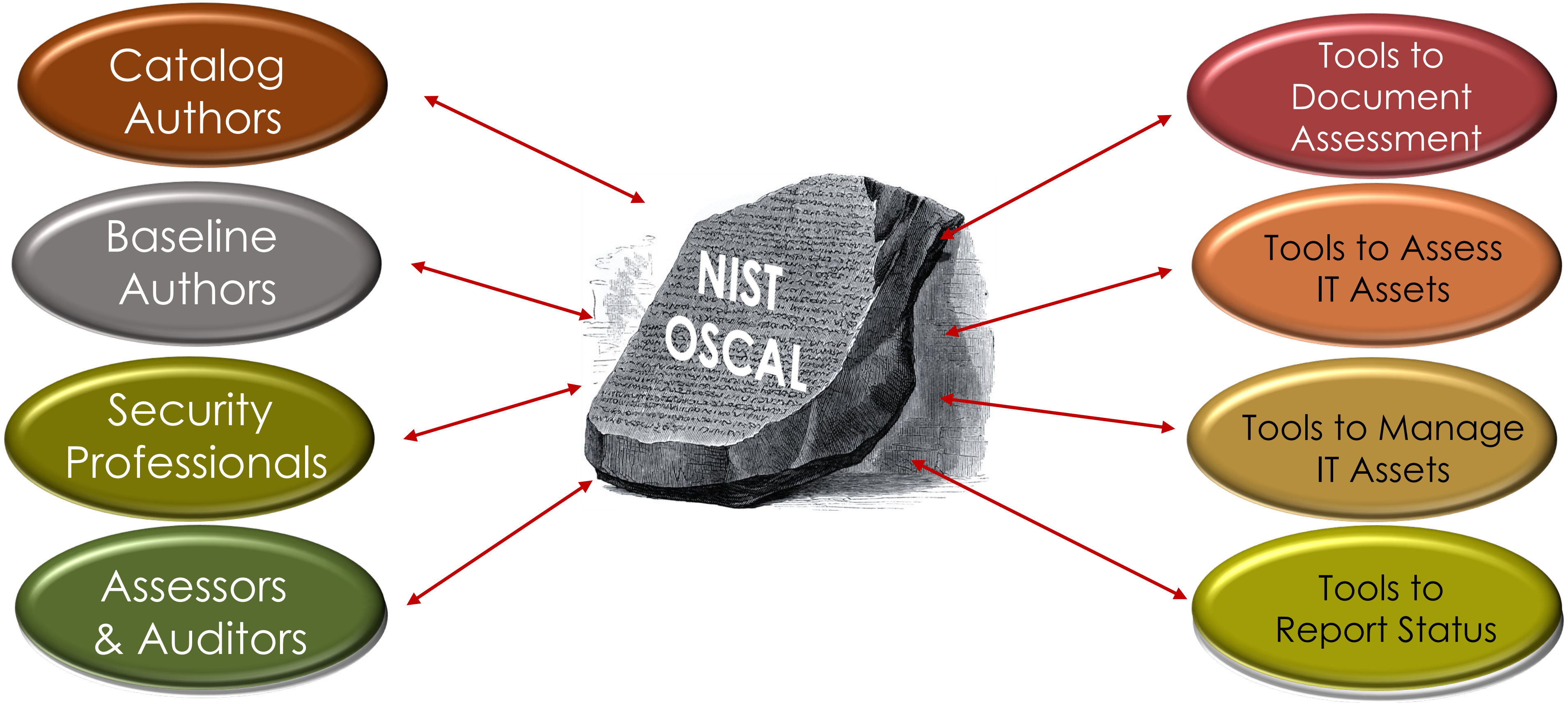
Why we care?

Today's challenges:

- Information technology is complex
- Security vulnerabilities are everywhere
- Regulatory frameworks are burdensome
- Risk management is hard
- Documentatio n becomes outdated fast

What was needed?

OSCAL is like a Rosetta Stone that enables tools and organizations to exchange information via automation

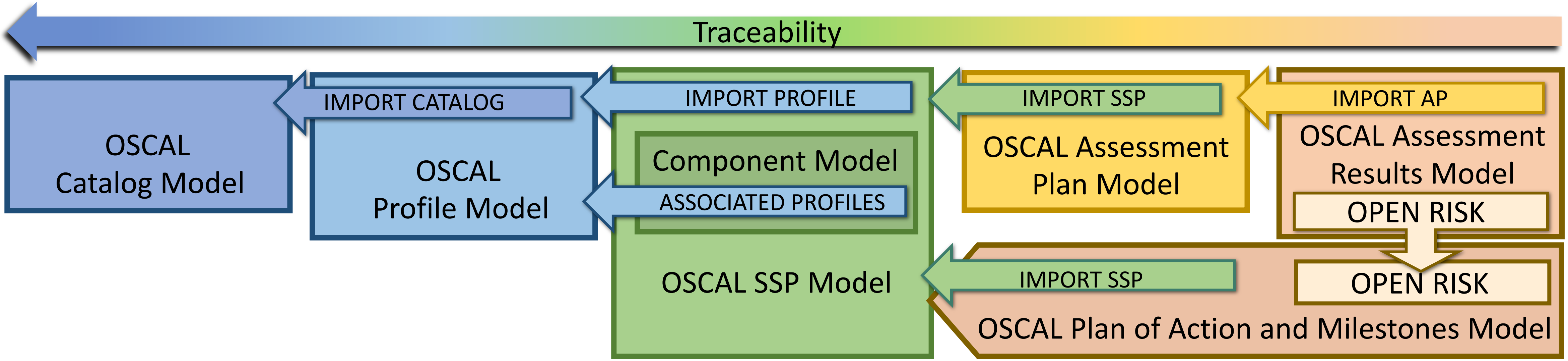


OSCAL sets the foundation for automation and interoperability

What is OSCAL?

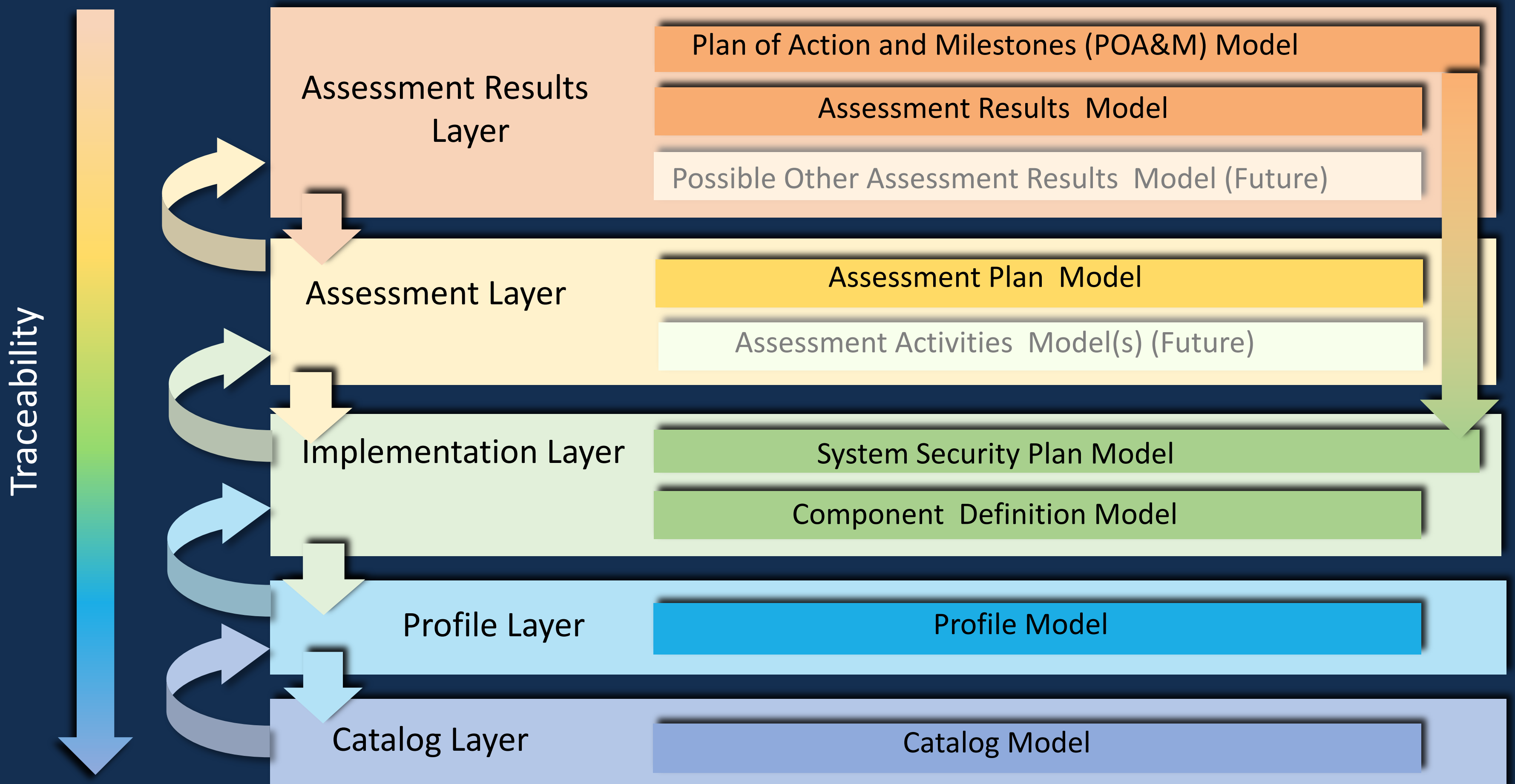
OSCAL is the result of NIST and FedRAMP collaboration

- ➢ **OSCAL provides** a common/single machine-readable *language*, expressed in XML, JSON and YAML for:
  - ❑ multiple compliance and risk management frameworks (e.g. SP 800-53, ISO/IEC 27001&2, COBIT 5)
  - ❑ software and service providers to express implementation guidance against security controls (Component definition)
  - ❑ sharing how security controls are implemented (System Security Plans [SSPs])
  - ❑ sharing security assessment plans (System Assessment Plans [SAPs])
  - ❑ sharing security assessment results/reports (System Assessment Results [SARs])
- ➢ **OSCAL enables** automated traceability from selection of security controls through implementation and assessment



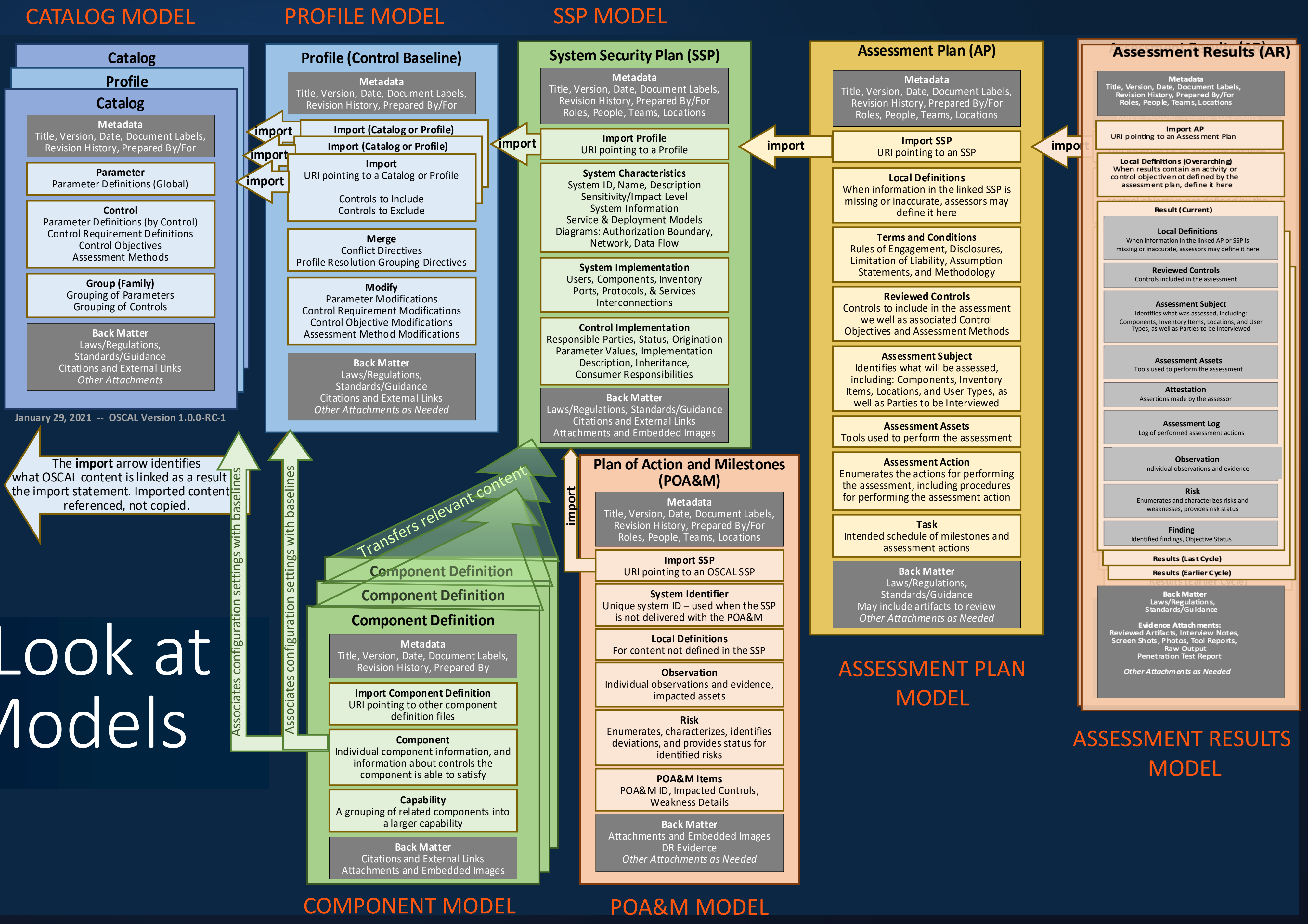
OSCAL 1.0.0 Architecture

Layers & Models



Traceability
Assessment Results Layer
Plan of Action and Milestones (POA&M) Model
Assessment Results Model
Possible Other Assessment Results Model (Future)
Assessment Layer
Assessment Plan Model
Assessment Activities Model(s) (Future)
Implementation Layer
System Security Plan Model
Component Definition Model
Profile Layer
Profile Model
Catalog Layer
Catalog Model

A Closer Look at OSCAL Models



CATALOG MODEL

Catalog

Profile

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

January 29, 2021 -- OSCAL Version 1.0.0-RC-1

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

PROFILE MODEL

Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

import

Import (Catalog or Profile)

import

Import (Catalog or Profile)

import

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

Associates configuration settings with baselines

Associates configuration settings with baselines

SSP MODEL

System Security Plan (SSP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

import

Import Profile
URI pointing to a Profile

System Characteristics
System ID, Name, Description
Sensitivity/Impact Level
System Information
Service & Deployment Models
Diagrams: Authorization Boundary, Network, Data Flow

System Implementation
Users, Components, Inventory
Ports, Protocols, & Services
Interconnections

Control Implementation
Responsible Parties, Status, Origination
Parameter Values, Implementation Description, Inheritance,
Consumer Responsibilities

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

Transfers relevant content

COMPONENT MODEL

Component Definition

Component Definition

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

POA&M MODEL

Plan of Action and Milestones (POA&M)

import

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates, characterizes, identifies deviations, and provides status for identified risks

POA&M Items
POA&M ID, Impacted Controls, Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

ASSESSMENT PLAN MODEL

Assessment Plan (AP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

import

Import SSP
URI pointing to an SSP

Local Definitions
When information in the linked SSP is missing or inaccurate, assessors may define it here

Terms and Conditions
Rules of Engagement, Disclosures, Limitation of Liability, Assumption Statements, and Methodology

Reviewed Controls
Controls to include in the assessment we well as associated Control Objectives and Assessment Methods

Assessment Subject
Identifies what will be assessed, including: Components, Inventory Items, Locations, and User Types, as well as Parties to be Interviewed

Assessment Assets
Tools used to perform the assessment

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

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

ASSESSMENT RESULTS MODEL

Assessment Results (AR)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For
Roles, People, Teams, Locations

import

Import AP
URI pointing to an Assessment Plan

Local Definitions (Overarching)
When results contain an activity or control objective not defined by the assessment plan, define it here

Result (Current)

Local Definitions
When information in the linked AP or SSP is missing or inaccurate, assessors may define it here

Reviewed Controls
Controls included in the assessment

Assessment Subject
Identifies what was assessed, including: Components, Inventory Items, Locations, and User Types, as well as Parties to be interviewed

Assessment Assets
Tools used to perform the assessment

Attestation
Assertions made by the assessor

Assessment Log
Log of performed assessment actions

Observation
Individual observations and evidence

Risk
Enumerates and characterizes risks and weaknesses, provides risk status

Finding
Identified findings, Objective Status

Results (Last Cycle)

Results (Earlier Cycle)

Back Matter
Laws/Regulations, Standards/Guidance

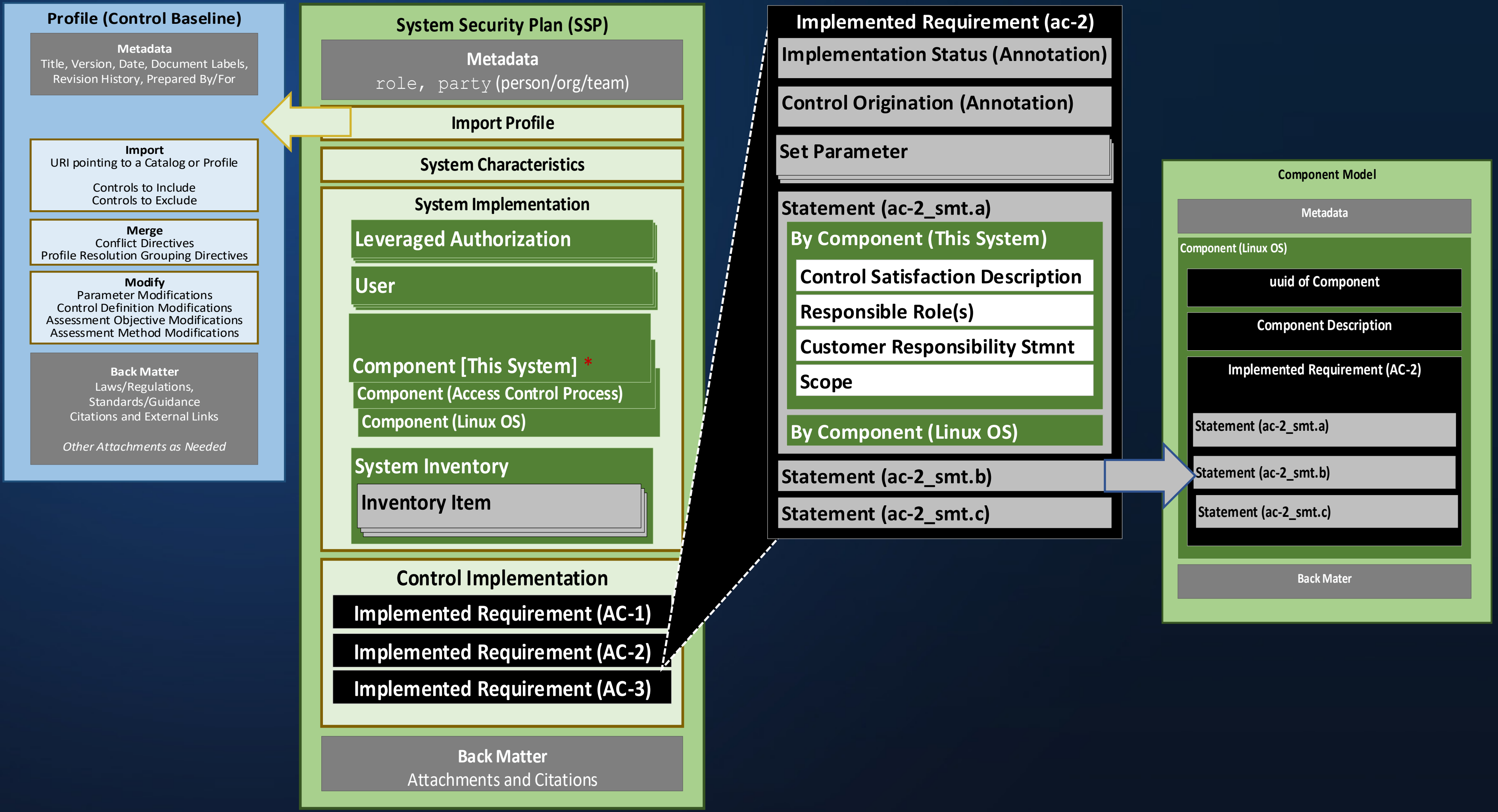
Evidence Attachments:
Reviewed Artifacts, Interview Notes, Screen Shots, Photos, Tool Reports, Raw Output
Penetration Test Report

Other Attachments as Needed

Where the Innovation Truly Starts:
The OSCAL Implementation Layer

OSCAL SSP:

- Imports a Profile identifying the controls
- Each control response is broken down to the individual components involved.
- Enables a more robust response to controls
- Example: The access control implementation that satisfies *AC-2, part a* is described separately for:
  - □ This System
  - □ The Access Control Procedure
  - □ A shared Application



Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

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 Definition Modifications
Assessment Objective Modifications
Assessment Method Modifications

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

Other Attachments as Needed

System Security Plan (SSP)

Metadata
`role`, `party` (person/org/team)

Import Profile

System Characteristics

System Implementation

Leveraged Authorization

User

Component [This System] *

Component (Access Control Process)

Component (Linux OS)

System Inventory

Inventory Item

Control Implementation

Implemented Requirement (AC-1)

Implemented Requirement (AC-2)

Implemented Requirement (AC-3)

Back Matter
Attachments and Citations

Implemented Requirement (ac-2)

Implementation Status (Annotation)

Control Origination (Annotation)

Set Parameter

Statement (ac-2_smt.a)

By Component (This System)

Control Satisfaction Description

Responsible Role(s)

Customer Responsibility Stmnt

Scope

By Component (Linux OS)

Statement (ac-2_smt.b)

Statement (ac-2_smt.c)

Component Model

Metadata

Component (Linux OS)

uuid of Component

Component Description

Implemented Requirement (AC-2)

Statement (ac-2_smt.a)

Statement (ac-2_smt.b)

Statement (ac-2_smt.c)

Back Mater

* Every SSP, must have a component representing the whole system.

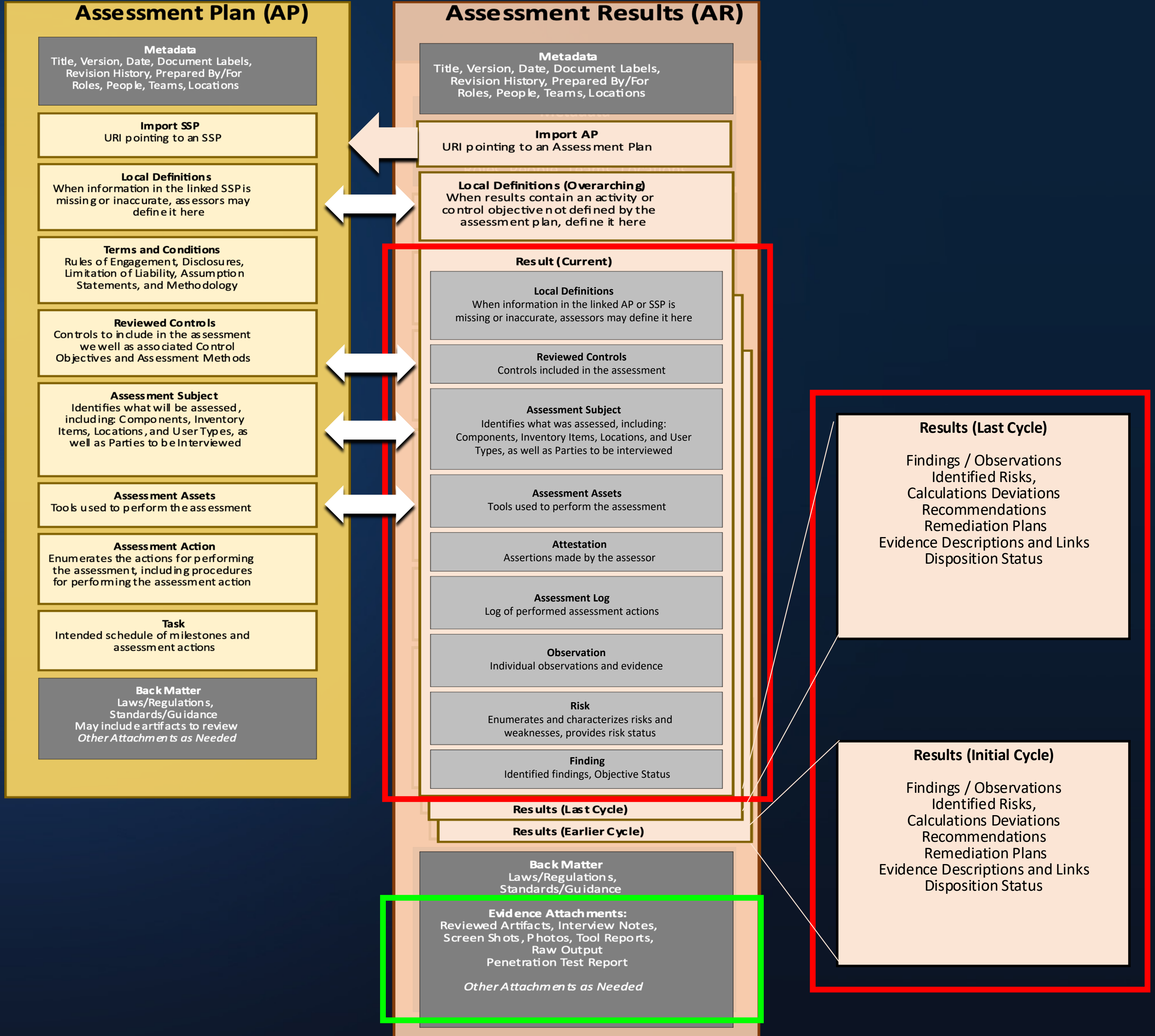
Assessment Plan (SAP) & Assessment Results (AR)

- ➢ OVERLAPING SYNTAX
- ➢ SIMILAR BUT DISTINCT PURPOSE
- ➢ 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

Planed activities ⟷ Actual activities



Assessment Plan (AP)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import SSP
URI pointing to an SSP

Local Definitions
When information in the linked SSP is missing or inaccurate, assessors may define it here

Terms and Conditions
Rules of Engagement, Disclosures, Limitation of Liability, Assumption Statements, and Methodology

Reviewed Controls
Controls to include in the assessment we well as associated Control Objectives and Assessment Methods

Assessment Subject
Identifies what will be assessed, including: Components, Inventory Items, Locations, and User Types, as well as Parties to be Interviewed

Assessment Assets
Tools used to perform the assessment

Assessment Action
Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task
Intended schedule of milestones and assessment actions

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

Assessment Results (AR)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import AP
URI pointing to an Assessment Plan

Local Definitions (Overarching)
When results contain an activity or control objective not defined by the assessment plan, define it here

Result (Current)

Local Definitions
When information in the linked AP or SSP is missing or inaccurate, assessors may define it here

Reviewed Controls
Controls included in the assessment

Assessment Subject
Identifies what was assessed, including: Components, Inventory Items, Locations, and User Types, as well as Parties to be interviewed

Assessment Assets
Tools used to perform the assessment

Attestation
Assertions made by the assessor

Assessment Log
Log of performed assessment actions

Observation
Individual observations and evidence

Risk
Enumerates and characterizes risks and weaknesses, provides risk status

Finding
Identified findings, Objective Status

Results (Last Cycle)

Results (Earlier Cycle)

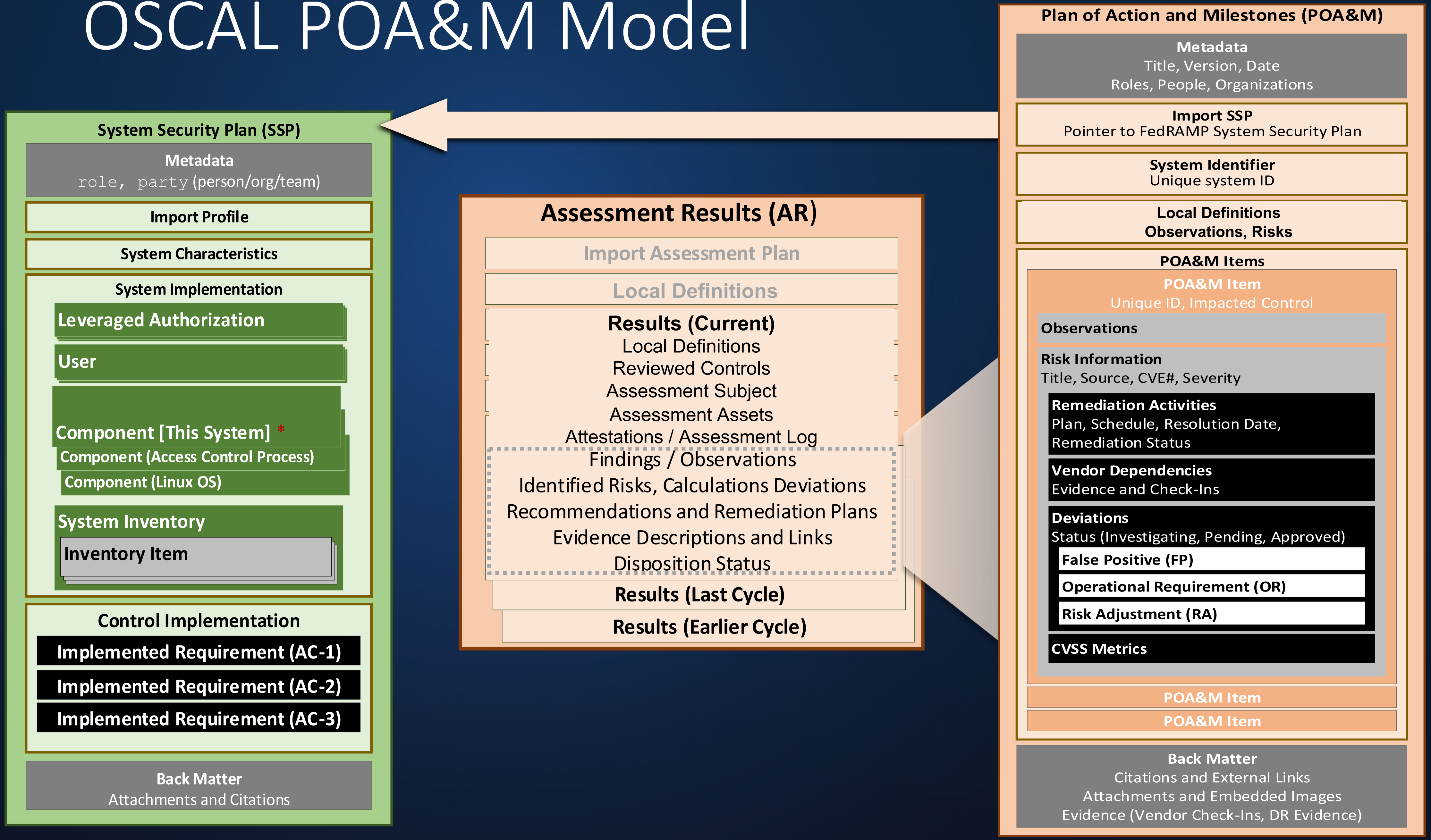
Back Matter
Laws/Regulations, Standards/Guidance

Evidence Attachments:
Reviewed Artifacts, Interview Notes, Screen Shots, Photos, Tool Reports, Raw Output
Penetration Test Report
Other Attachments as Needed

Results (Last Cycle)
Findings / Observations
Identified Risks,
Calculations Deviations
Recommendations
Remediation Plans
Evidence Descriptions and Links
Disposition Status

Results (Initial Cycle)
Findings / Observations
Identified Risks,
Calculations Deviations
Recommendations
Remediation Plans
Evidence Descriptions and Links
Disposition Status

OSCAL POA&M Model



System Security Plan (SSP)

Metadata
`role, party` (person/org/team)

Import Profile

System Characteristics

System Implementation

- Leveraged Authorization
- User
- Component [This System] *
- Component (Access Control Process)
- Component (Linux OS)
- System Inventory
  - Inventory Item

Control Implementation

- Implemented Requirement (AC-1)
- Implemented Requirement (AC-2)
- Implemented Requirement (AC-3)

Back Matter
Attachments and Citations

Assessment Results (AR)

Import Assessment Plan

Local Definitions

Results (Current)
Local Definitions
Reviewed Controls
Assessment Subject
Assessment Assets
Attestations / Assessment Log
Findings / Observations
Identified Risks, Calculations Deviations
Recommendations and Remediation Plans
Evidence Descriptions and Links
Disposition Status

Results (Last Cycle)

Results (Earlier Cycle)

Plan of Action and Milestones (POA&M)

Metadata
Title, Version, Date
Roles, People, Organizations

Import SSP
Pointer to FedRAMP System Security Plan

System Identifier
Unique system ID

Local Definitions
Observations, Risks

POA&M Items

POA&M Item
Unique ID, Impacted Control

Observations

Risk Information
Title, Source, CVE#, Severity

Remediation Activities
Plan, Schedule, Resolution Date,
Remediation Status

Vendor Dependencies
Evidence and Check-Ins

Deviations
Status (Investigating, Pending, Approved)

- False Positive (FP)
- Operational Requirement (OR)
- Risk Adjustment (RA)

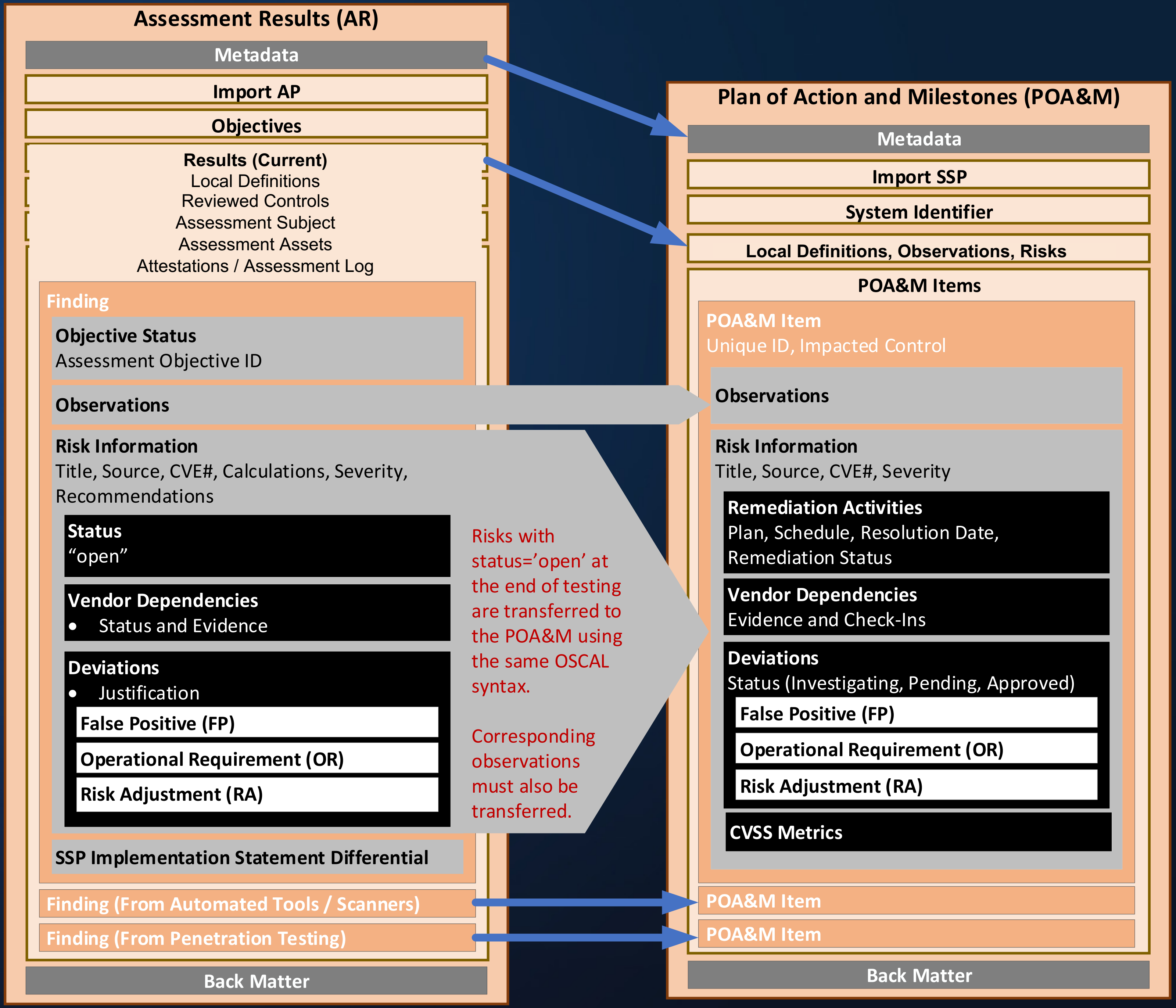
CVSS Metrics

POA&M Item

POA&M Item

Back Matter
Citations and External Links
Attachments and Embedded Images
Evidence (Vendor Check-Ins, DR Evidence)

Assessment Results & POA&Ms Overlapping Syntax



Assessment Results (AR)

Metadata

Import AP

Objectives

Results (Current)
Local Definitions
Reviewed Controls
Assessment Subject
Assessment Assets
Attestations / Assessment Log

Finding

Objective Status
Assessment Objective ID

Observations

Risk Information
Title, Source, CVE#, Calculations, Severity, Recommendations

Status
“open”

Vendor Dependencies
- Status and Evidence

Deviations
- Justification

False Positive (FP)

Operational Requirement (OR)

Risk Adjustment (RA)

SSP Implementation Statement Differential

Finding (From Automated Tools / Scanners)

Finding (From Penetration Testing)

Back Matter

Risks with status=’open’ at the end of testing are transferred to the POA&M using the same OSCAL syntax.

Corresponding observations must also be transferred.

Plan of Action and Milestones (POA&M)

Metadata

Import SSP

System Identifier

Local Definitions, Observations, Risks

POA&M Items

POA&M Item
Unique ID, Impacted Control

Observations

Risk Information
Title, Source, CVE#, Severity

Remediation Activities
Plan, Schedule, Resolution Date, Remediation Status

Vendor Dependencies
Evidence and Check-Ins

Deviations
Status (Investigating, Pending, Approved)

False Positive (FP)

Operational Requirement (OR)

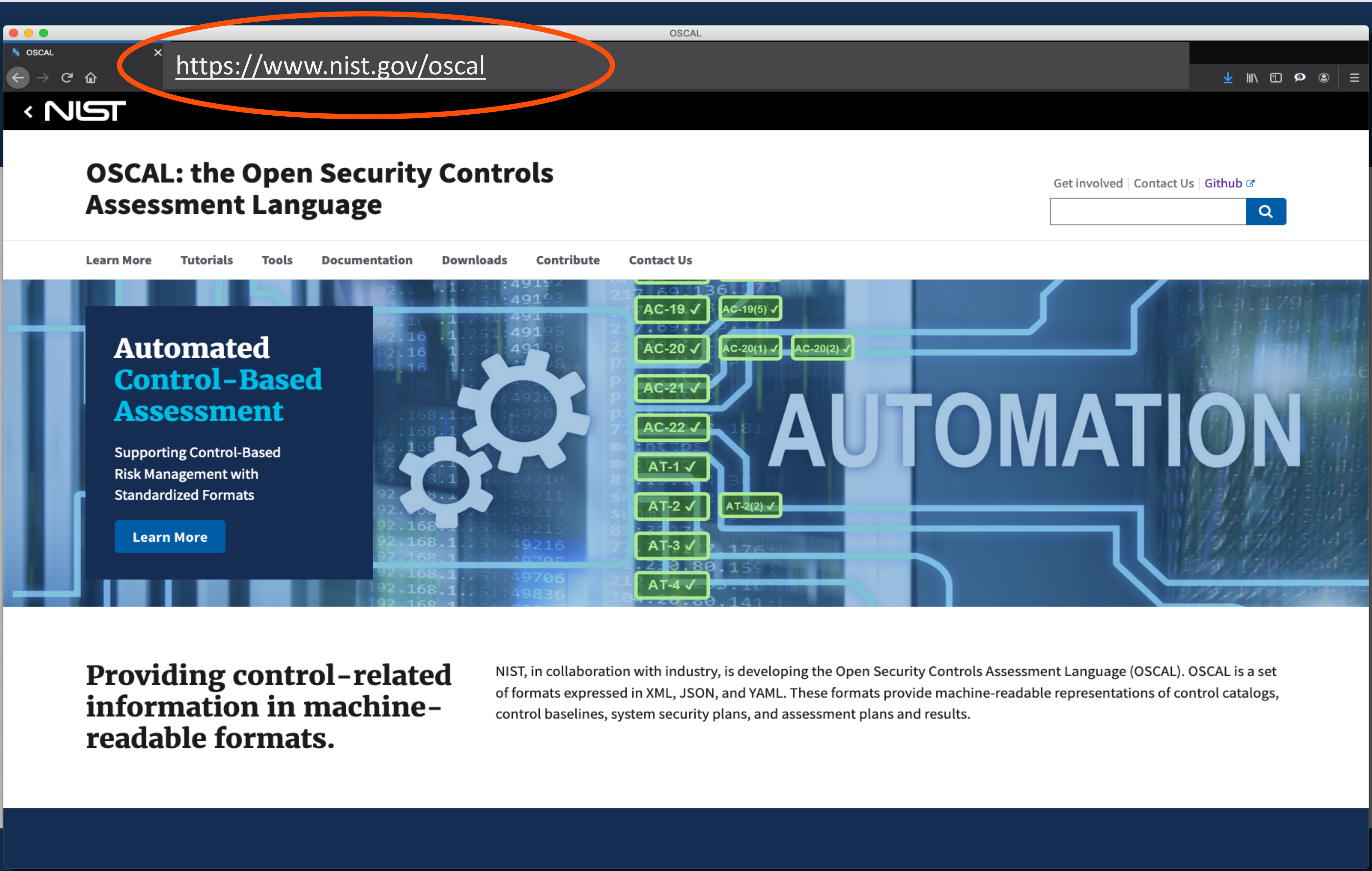
Risk Adjustment (RA)

CVSS Metrics

POA&M Item

POA&M Item

Back Matter



https://www.nist.gov/oscal

OSCAL: the Open Security Controls Assessment Language

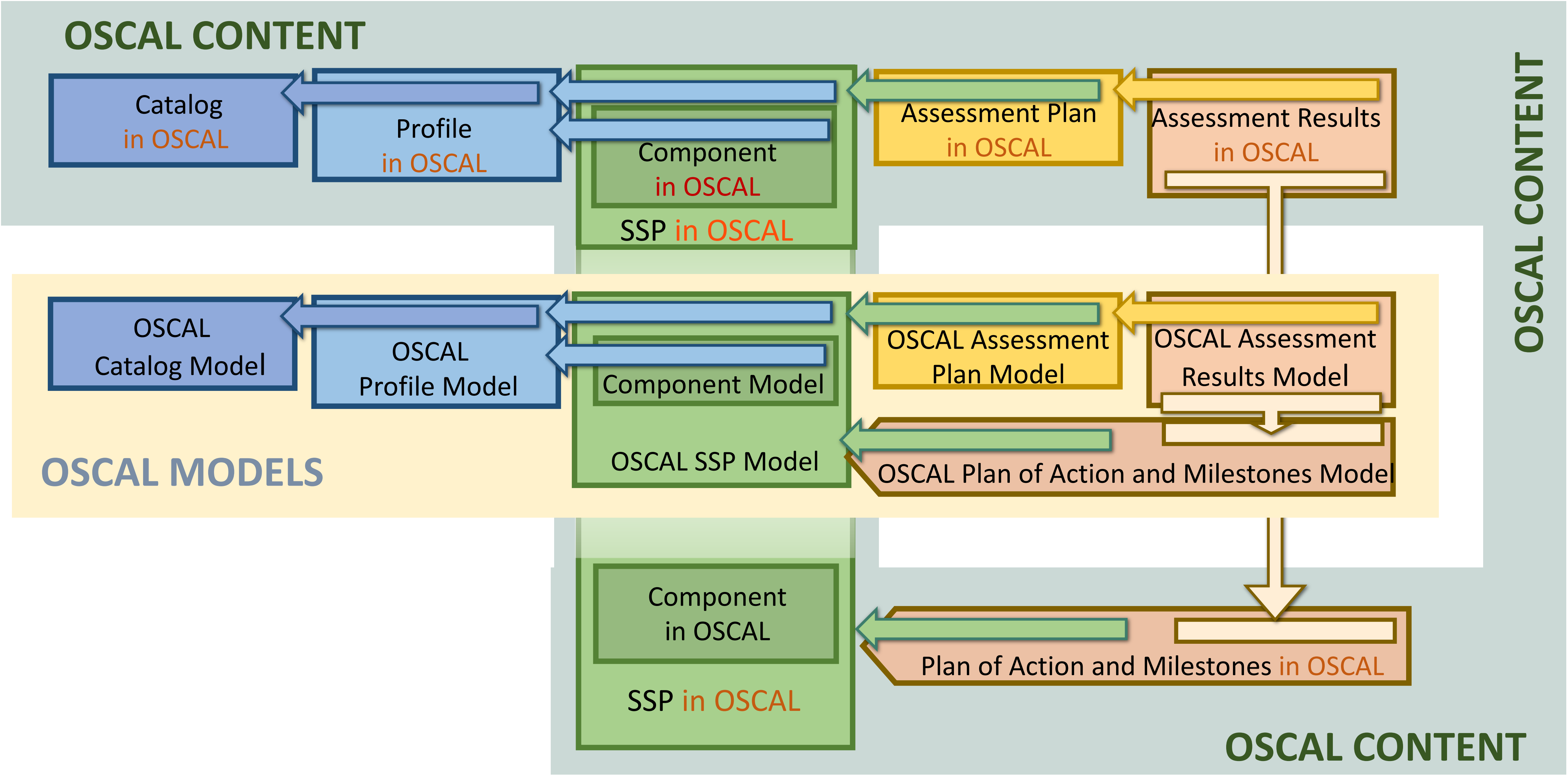
Automated Control-Based Assessment

Supporting Control-Based Risk Management with Standardized Formats

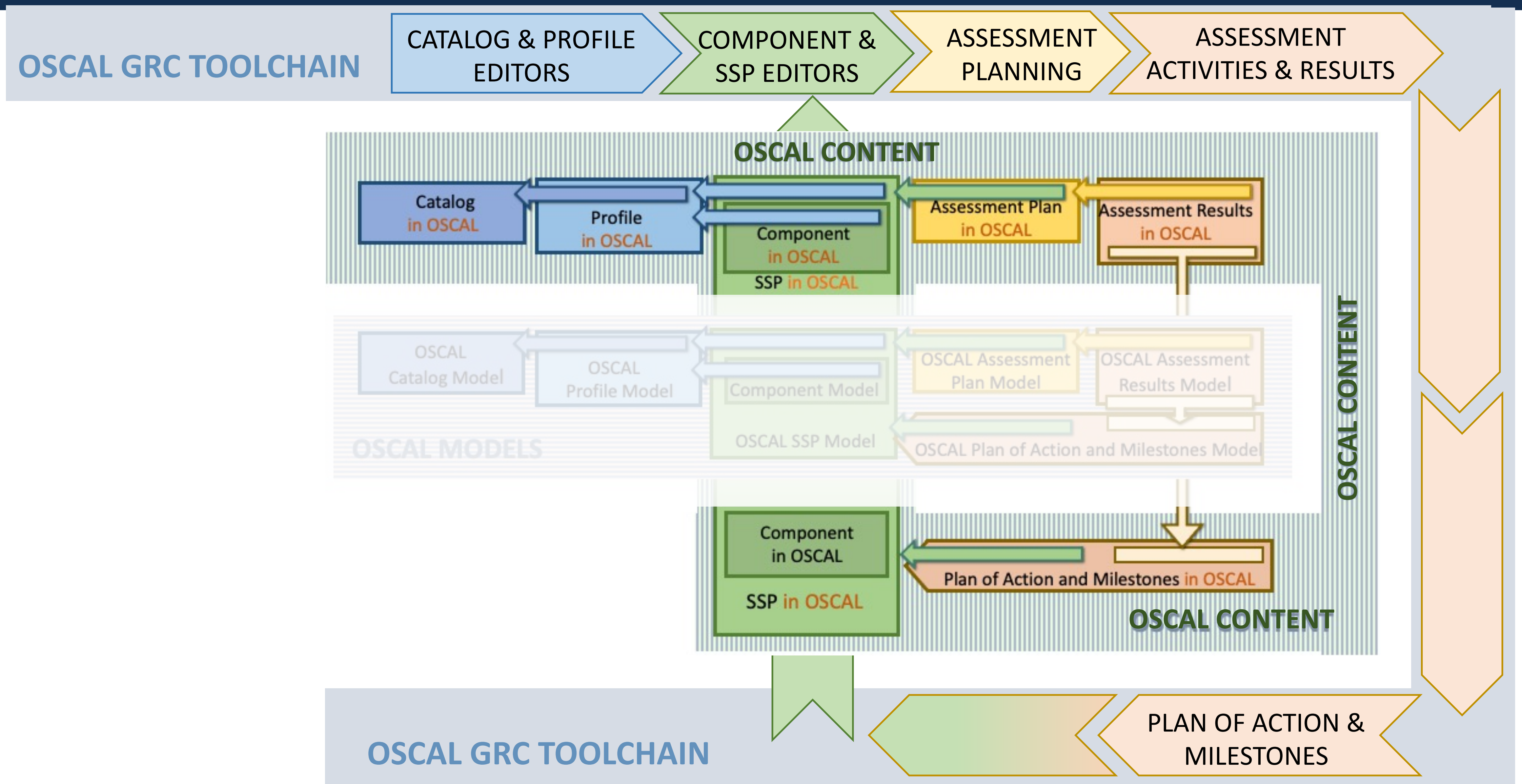
Providing control-related information in machine-readable formats.

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 vs. OSCAL Content



OSCAL Content vs OSCAL Tools



OSCAL GRC TOOLCHAIN

CATALOG & PROFILE EDITORS

COMPONENT & SSP EDITORS

ASSESSMENT PLANNING

ASSESSMENT ACTIVITIES & RESULTS

OSCAL CONTENT

Catalog in OSCAL

Profile in OSCAL

Component in OSCAL

SSP in OSCAL

Assessment Plan in OSCAL

Assessment Results in OSCAL

OSCAL Catalog Model

OSCAL Profile Model

Component Model

OSCAL SSP Model

OSCAL Assessment Plan Model

OSCAL Assessment Results Model

OSCAL Plan of Action and Milestones Model

OSCAL MODELS

OSCAL CONTENT

Component in OSCAL

SSP in OSCAL

Plan of Action and Milestones in OSCAL

OSCAL CONTENT

PLAN OF ACTION & MILESTONES

OSCAL GRC TOOLCHAIN

OSCAL CONTENT (XML, JSON, YAML) Catalogs and Profiles

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

- examples
- fedramp.gov
- nist.gov/SP800-53
- oscal @ d26e3b3
- src

Maintainer	OSCAL Information		Source Documents
NIST	SP 800-53 Catalog	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 NIST Low Baseline	Rev 4	NIST SP 800-53 Rev4
	SP 800-53 NIST Moderate Baseline	Rev 4	NIST SP 800-53 Rev4
	SP 800-53 NIST High Baseline	Rev 4	NIST SP 800-53 Rev4
	SP 800-53 NIST Resolved Low Baseline	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 NIST Resolved Moderate Baseline	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 NIST Resolved High Baseline	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 Catalog	Rev 5	NIST SP 800-53 Rev5
	SP 800-53 NIST Low Baseline	Rev 5	NIST SP 800-53 Rev5B
	SP 800-53 NIST Moderate Baseline	Rev 5	NIST SP 800-53 Rev5B
	SP 800-53 NIST High Baseline	Rev 5	NIST SP 800-53 Rev5B
	SP 800-53 NIST Privacy Baseline	Rev 5	NIST SP 800-53 Rev5B

OSCAL (XML, JSON, YAML) Examples

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

- ➢ examples
- ➢ fedramp.gov
- ➢ nist.gov/SP800-53
- ➢ oscal @ d26e3b3
- ➢ src

❑ The content of the 'examples' directory is as follows:

- ➢ catalog: This directory contains sample content for the OSCAL catalog model.
- ➢ component-definition: This directory contains sample content for the OSCAL component definition model.
- ➢ ssp: This directory contains sample content for the OSCAL system security plan (SSP) model.

❑ Examples do not represent real data

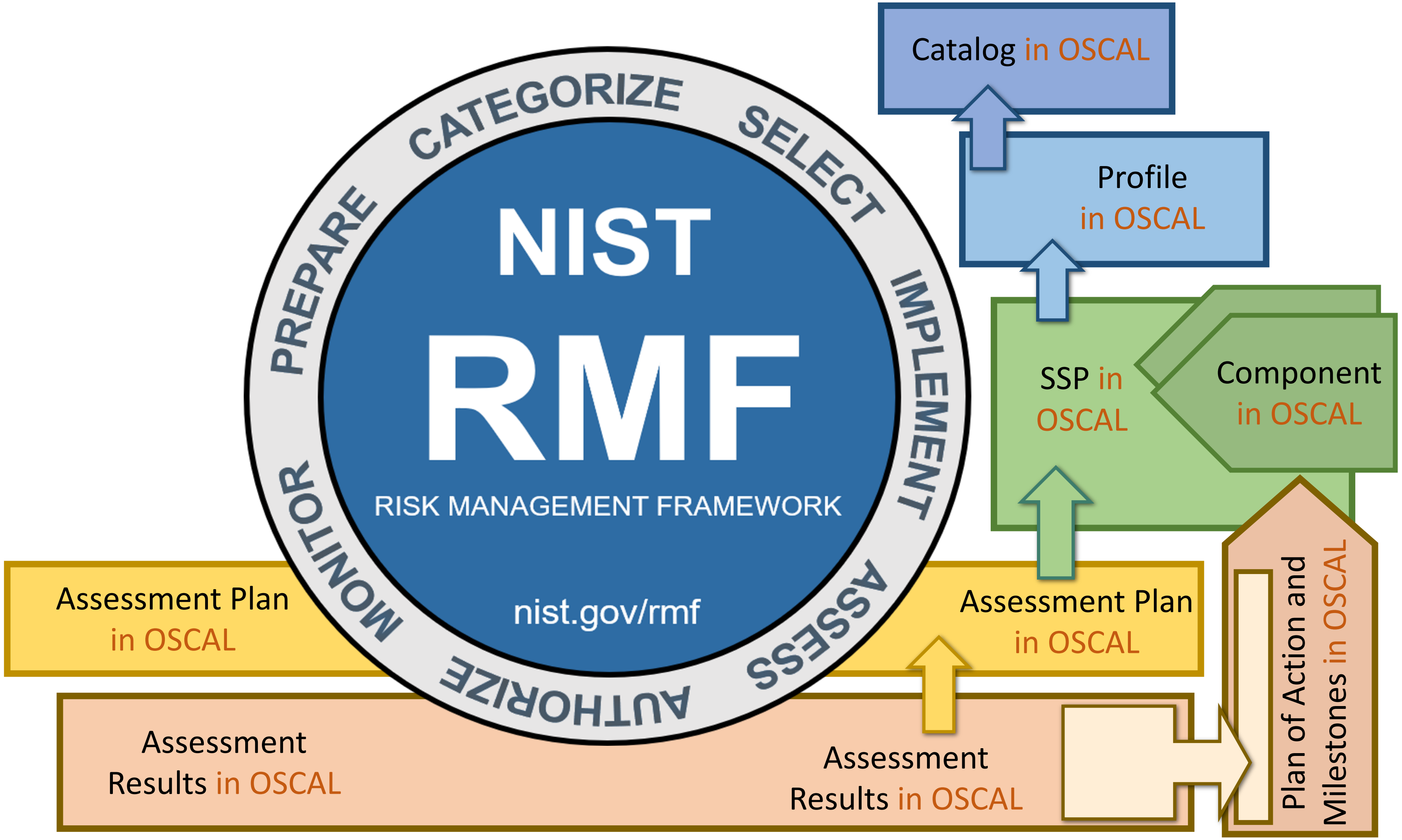
FedRAMP OSCAL (XML, JSON and YAML) Profiles

https://github.com/GSA/fedramp-automation:

- assets
- baselines
- documents
- oscal @ 5581a8e
- resources
- src
- templates

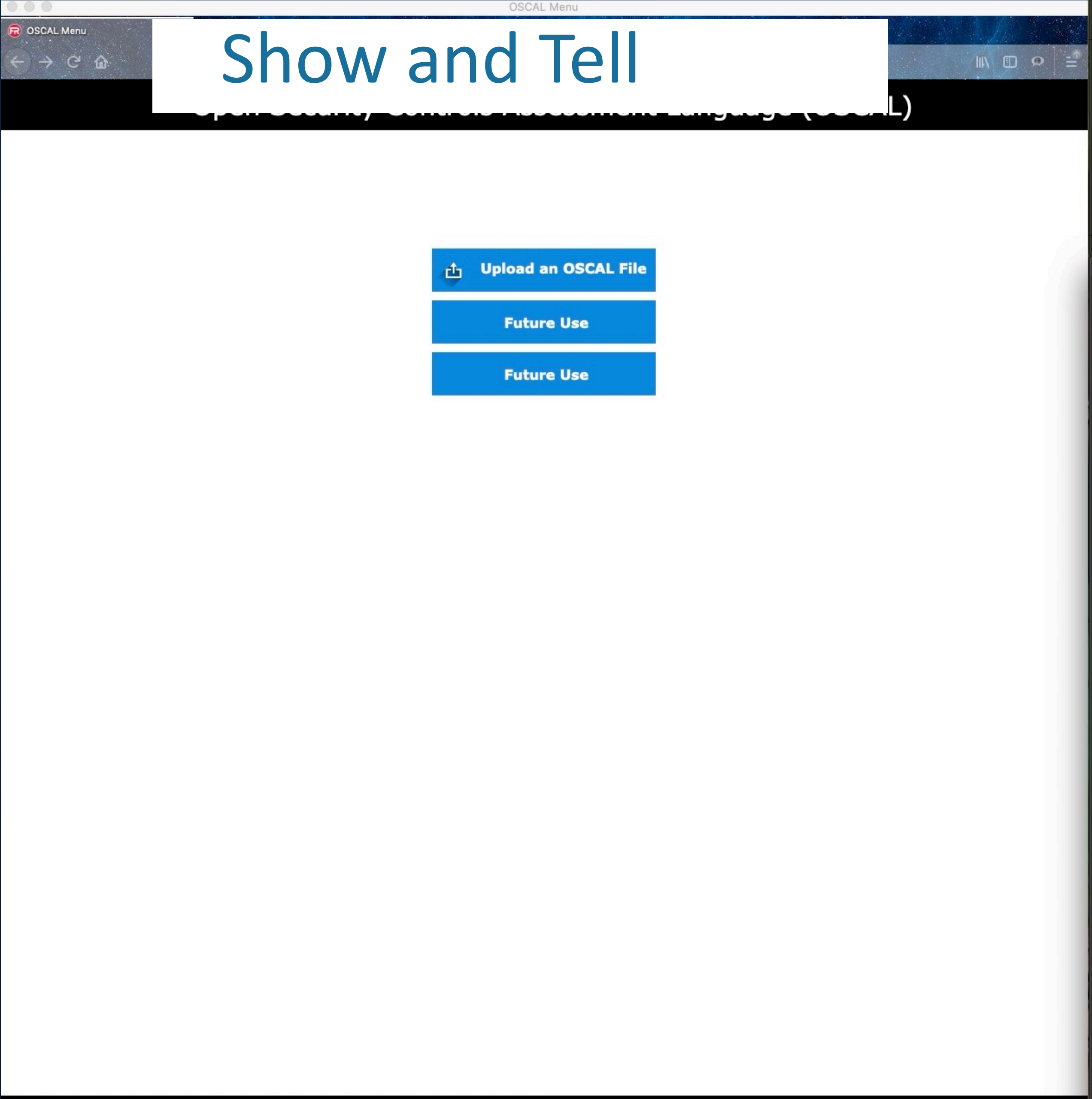
Maintainer	OSCAL Information		Source Documents
FedRAMP	SP 800-53 FedRAMP Low Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Moderate Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP High Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Tailored Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Low Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Moderate Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved High Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Tailored Baseline	Rev 4	FedRAMP Security Controls Baselines

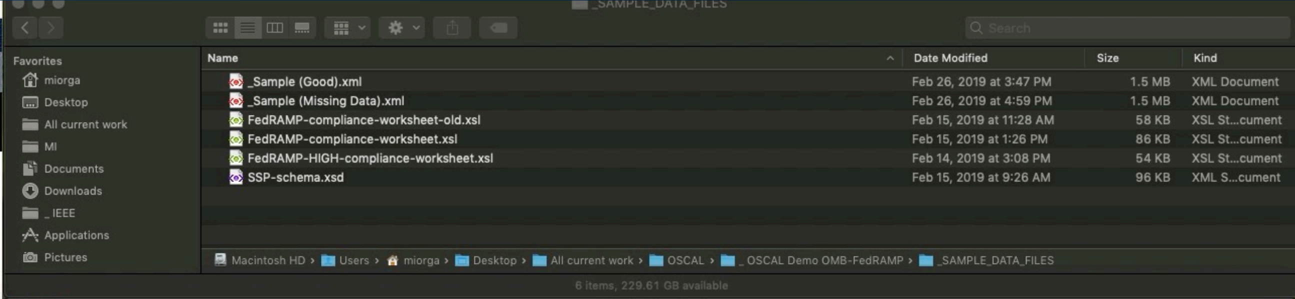
OSCAL Content & Risk Management Framework



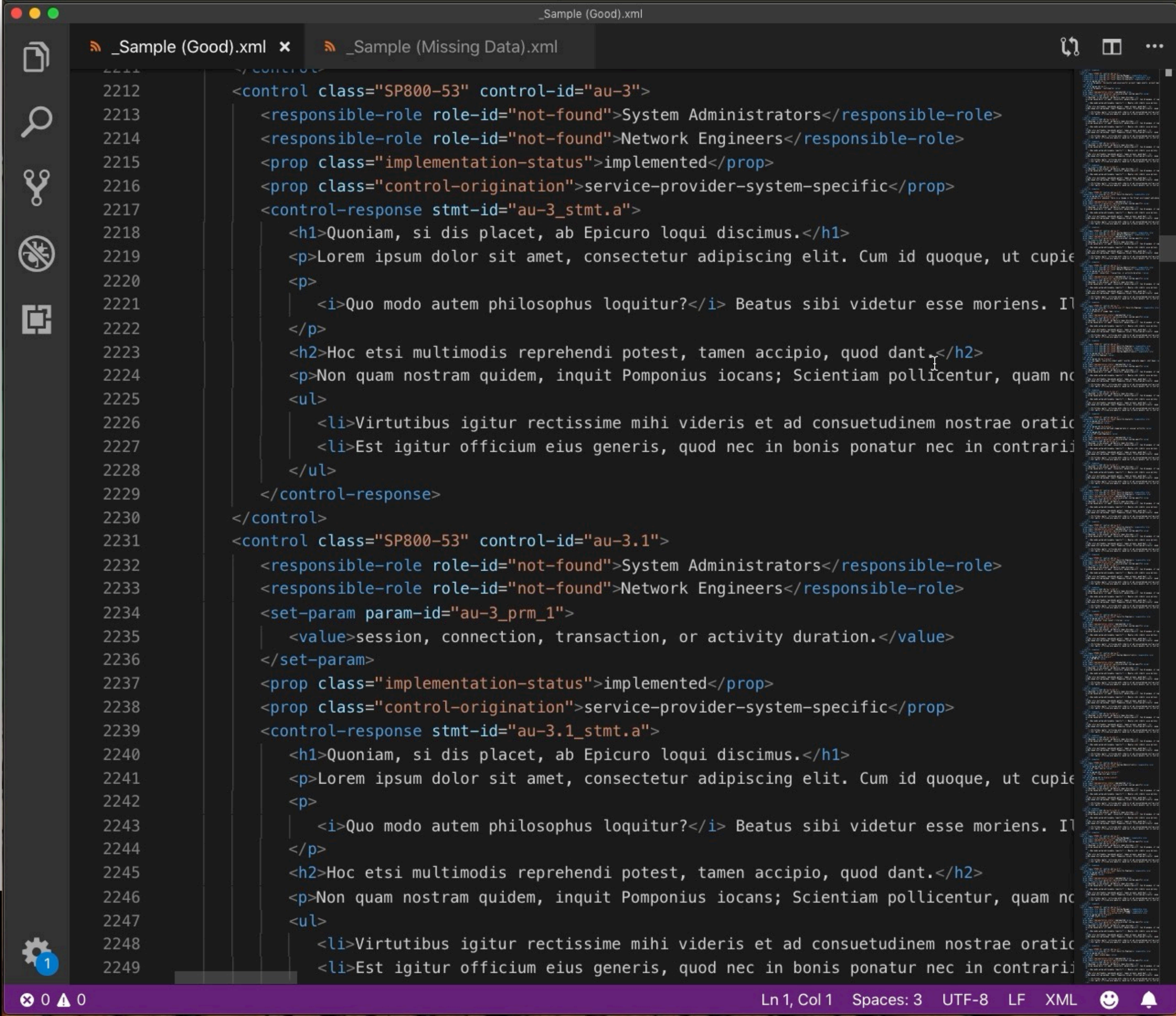
Brief Demo

Show and Tell




_SAMPLE_DATA_FILES
Favorites
miorga
Desktop
All current work
MI
Documents
Downloads
_ IEEE
Applications
Pictures
Macintosh HD › Users › miorga › Desktop › All current work › OSCAL › _ OSCAL Demo OMB-FedRAMP › _SAMPLE_DATA_FILES
6 items, 229.61 GB available

Name	Date Modified	Size	Kind
_Sample (Good).xml	Feb 26, 2019 at 3:47 PM	1.5 MB	XML Document
_Sample (Missing Data).xml	Feb 26, 2019 at 4:59 PM	1.5 MB	XML Document
FedRAMP-compliance-worksheet-old.xsl	Feb 15, 2019 at 11:28 AM	58 KB	XSL St...cument
FedRAMP-compliance-worksheet.xsl	Feb 15, 2019 at 1:26 PM	86 KB	XSL St...cument
FedRAMP-HIGH-compliance-worksheet.xsl	Feb 14, 2019 at 3:08 PM	54 KB	XSL St...cument
SSP-schema.xsd	Feb 15, 2019 at 9:26 AM	96 KB	XML S...cument

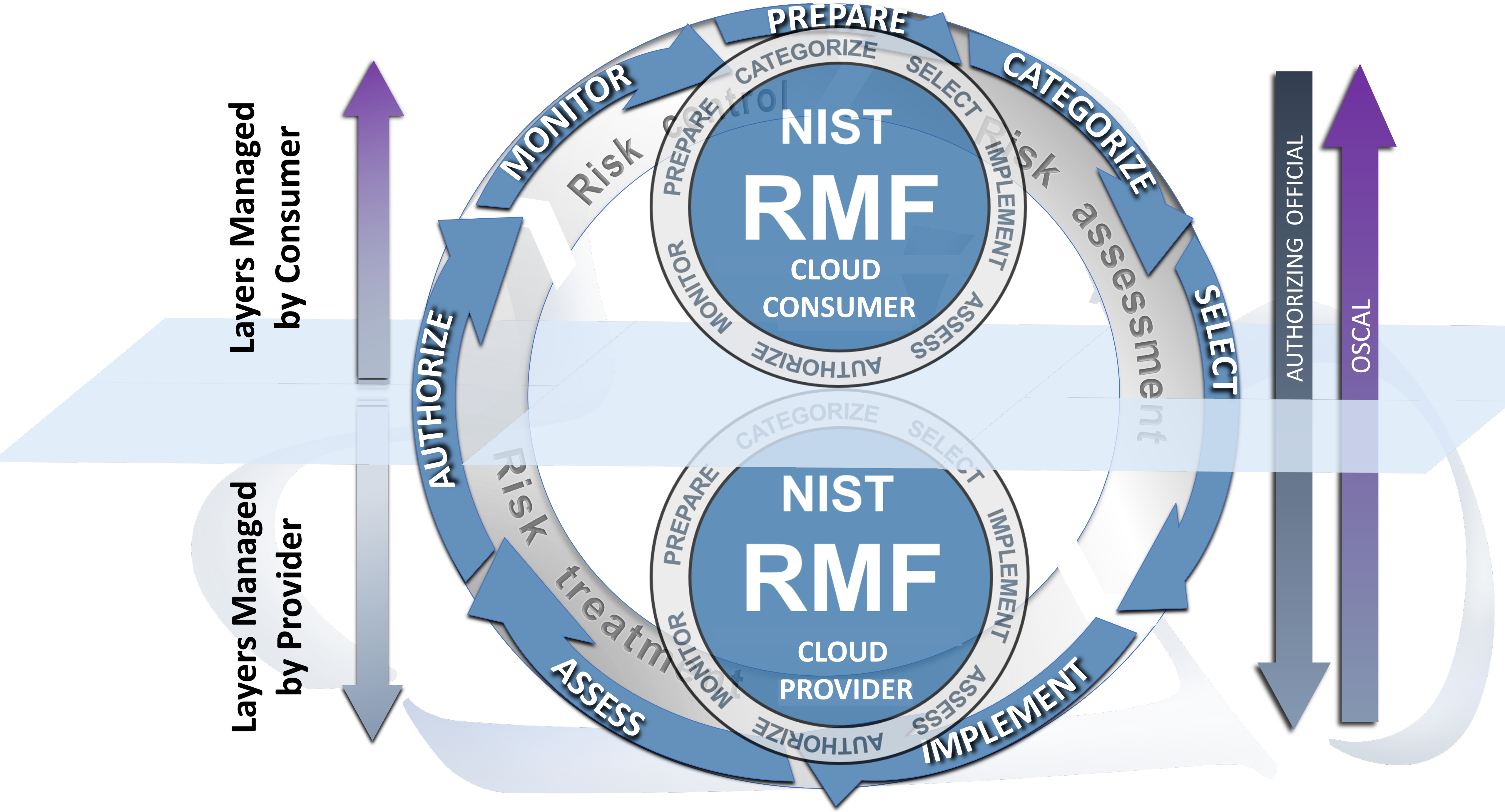


```
<control class="SP800-53" control-id="au-3">
   <responsible-role role-id="not-found">System Administrators</responsible-role>
   <responsible-role role-id="not-found">Network Engineers</responsible-role>
   <prop class="implementation-status">implemented</prop>
   <prop class="control-origination">service-provider-system-specific</prop>
   <control-response stmt-id="au-3_stmt.a">
      <h1>Quoniam, si dis placet, ab Epicuro loqui discimus.</h1>
      <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cum id quoque, ut cupie
      <p>
         <i>Quo modo autem philosophus loquitur?</i> Beatus sibi videtur esse moriens. Il
      </p>
      <h2>Hoc etsi multimodis reprehendi potest, tamen accipio, quod dant.</h2>
      <p>Non quam nostram quidem, inquit Pomponius iocans; Scientiam pollicentur, quam nc
      <ul>
         <li>Virtutibus igitur rectissime mihi videris et ad consuetudinem nostrae oratic
         <li>Est igitur officium eius generis, quod nec in bonis ponatur nec in contrari
      </ul>
   </control-response>
</control>
<control class="SP800-53" control-id="au-3.1">
   <responsible-role role-id="not-found">System Administrators</responsible-role>
   <responsible-role role-id="not-found">Network Engineers</responsible-role>
   <set-param param-id="au-3_prm_1">
      <value>session, connection, transaction, or activity duration.</value>
   </set-param>
   <prop class="implementation-status">implemented</prop>
   <prop class="control-origination">service-provider-system-specific</prop>
   <control-response stmt-id="au-3.1_stmt.a">
      <h1>Quoniam, si dis placet, ab Epicuro loqui discimus.</h1>
      <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cum id quoque, ut cupie
      <p>
         <i>Quo modo autem philosophus loquitur?</i> Beatus sibi videtur esse moriens. Il
      </p>
      <h2>Hoc etsi multimodis reprehendi potest, tamen accipio, quod dant.</h2>
      <p>Non quam nostram quidem, inquit Pomponius iocans; Scientiam pollicentur, quam nc
      <ul>
         <li>Virtutibus igitur rectissime mihi videris et ad consuetudinem nostrae oratic
         <li>Est igitur officium eius generis, quod nec in bonis ponatur nec in contrari
```

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

FedRAMP
Federal Risk and Authorization Management Program

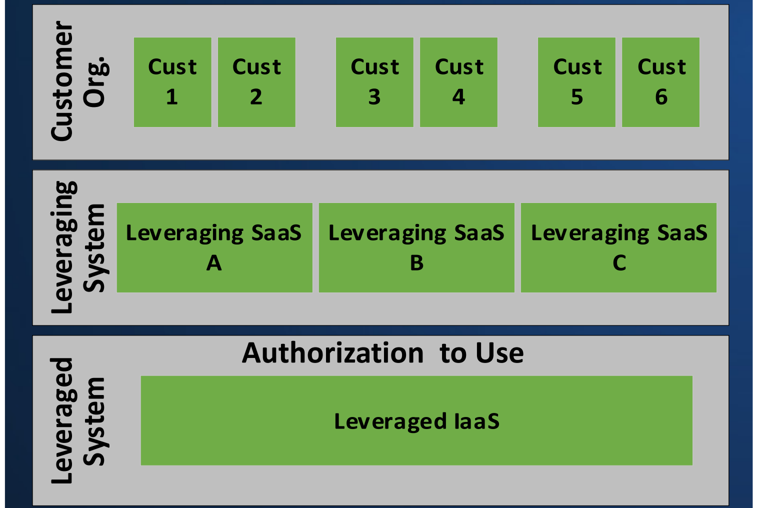
Authorization to Use & Common Control Authorization



Layers Managed
by Consumer
Layers Managed
by Provider
PREPARE
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
Risk control
Risk assessment
Risk treatment
NIST
RMF
CLOUD
CONSUMER
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE
NIST
RMF
CLOUD
PROVIDER
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE
AUTHORIZING OFFICIAL
OSCAL

Common Control Authorization & **Authorization to Use**

Yes



Customer Org.

Cust 1 | Cust 2 | Cust 3 | Cust 4 | Cust 5 | Cust 6

Leveraging System

Leveraging SaaS A | Leveraging SaaS B | Leveraging SaaS C

Leveraged System

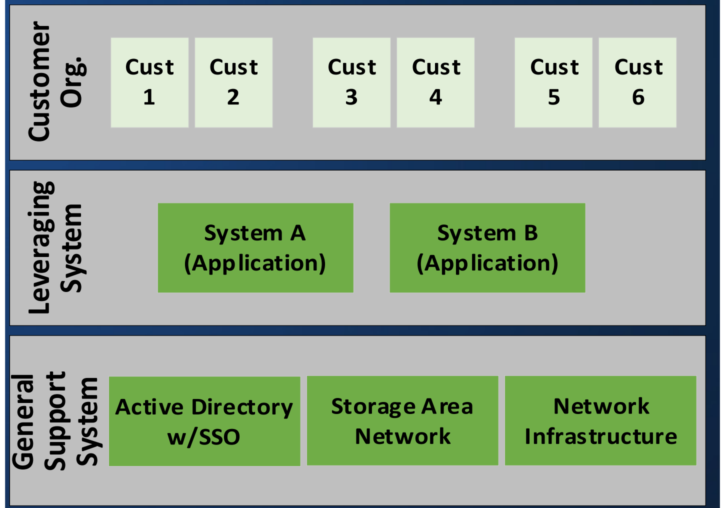
Authorization to Use

Leveraged IaaS

Cloud (SaaS on IaaS)

Cloud: Several SaaS systems running on a separately authorized IaaS.

Yes



Customer Org.

Cust 1 | Cust 2 | Cust 3 | Cust 4 | Cust 5 | Cust 6

Leveraging System

System A (Application) | System B (Application)

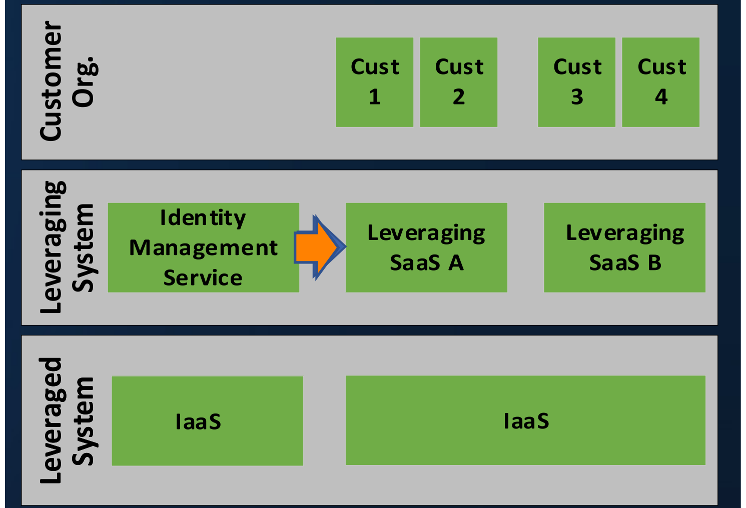
General Support System

Active Directory w/SSO | Storage Area Network | Network Infrastructure

Data Center (System on GSS)

Data Center: Several systems relying on a separately authorized storage array or other general support system (GSS)

No



Customer Org.

Cust 1 | Cust 2 | Cust 3 | Cust 4

Leveraging System

Identity Management Service → Leveraging SaaS A | Leveraging SaaS B

Leveraged System

IaaS | IaaS

External Service or Interconnection

Interconnections or External Services are not leveraged authorizations

- Even if they have an authorization
- SaaS A handles the Identity Management Service as a system component

OSCAL supports this, just not as a L.A.

Authorization-to-Use: OSCAL Support

Scenario 1: OSCAL SSP / With Access

The leveraged system is using an OSCAL SSP; and the leveraging system is permitted to access it.

No CRM/SSRM is needed.

Preferred approach!

Completed

Scenario 2: OSCAL SSP / No Access

The leveraged system is using an OSCAL SSP; however,

the leveraging system is not permitted to access it.

An OSCAL CRM/SSRM is used.

Typical FedRAMP Scenario

Post OSCAL 1.0.0

Scenario 3: Legacy SSP

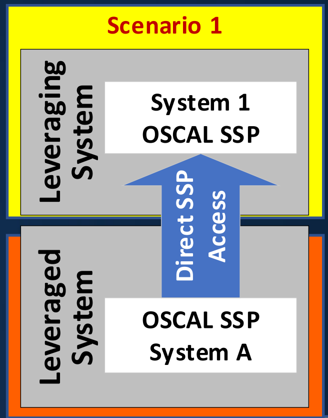
A leveraged system is still using a legacy SSP.

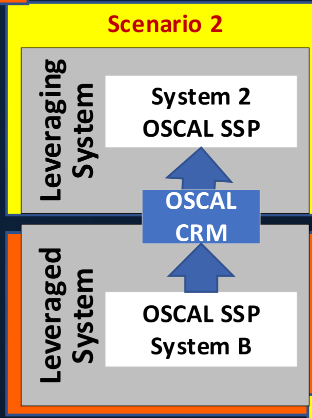
A legacy Customer Responsibility Matrix (CRM) or System Security Responsibility Matrix (SSRM) are used/available.

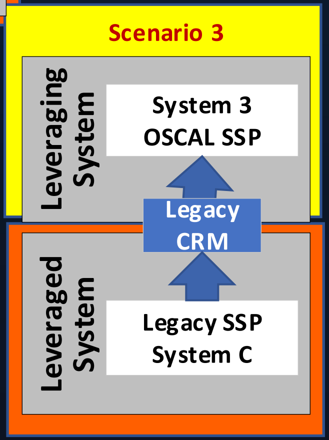
Transition scenario for an imperfect world

Post OSCAL 1.0.0

Three Scenarios







OSCAL content is for tools to consume!

Humans can see the information in nice html or pdf format using simple transformations over OSCAL content.

Example OSCAL Catalog transformed to HTML:

https://github.com/usnistgov/oscal-tools/blob/master/xslt/publish/generic-preview/oscal_catalog_html.xsl

Publicly Available Resources

Documentation:

Catalog, Profile, Component, SSP, SAP, SAR, POA&M:
https://pages.nist.gov/OSCAL/documentation/

Example:

Generic examples:
https://github.com/usnistgov/oscal-content/tree/master/examples

NIST SP 800-53 R4 and Rev5 catalog and baselines (XML & JSON):
https://github.com/usnistgov/oscal-content/tree/master/nist.gov/SP800-53

FedRAMP Automation:

FedRAMP

Repository (FedRAMP catalog and baselines (XML & JSON) included) :
https://github.com/GSA/fedramp-automation

https://www.fedramp.gov/using-the-fedramp-oscal-resources-and-templates/

Tools

OSCAL Java Library: https://github.com/usnistgov/liboscal-java
XSLT Tooling: https://github.com/usnistgov/oscal-tools/tree/master/xslt
OSCAL Kit: https://github.com/docker/oscalkit
OSCAL GUI: https://github.com/brianrufgsa/OSCAL-GUI
OMB'S OPAL: OSCAL Policy Administration Library (OPAL): https://github.com/EOP-OMB/opal

Please visit: OSCAL Club:oscal-club/**awesome-oscal**:
https://github.com/oscal-club/awesome-oscal

OSCAL Adopters

FedRAMP

noblis

ATO as a SERVICE™

MEDINA

Telos®

IBM Research

- □ FedRAMP
- □ Noblis
- □ HHS CMS
- □ National Renewable Energy Lab
- □ GovReady
- □ C2 Labs
- □ cFocus Software
- □ Shujinko
- □ Robers Bosch (EU|Germany)
- □ Telos

- □ Booz Allen Hamilton
- □ AWS
- □ Microsoft
- □ Coalfire
- □ Kratos
- □ eMASS
- □ CSAM
- □ Volant Associates, LLC
- □ Salesforce
- □ Oracle

Booz | Allen | Hamilton®

aws

KRATOS®
READY FOR WHAT'S NEXT™

salesforce

ORACLE

Questions?

Contact us at: oscal@nist.gov

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

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

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

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

Thank you!