Open Security Controls Assessment Language
OSCAL

Dr. Michaela Iorga,
OSCAL Strategic Outreach Director

February 17, 2022

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

Why are we all here today?

Because we are faced with the same challenges:

Information technology is complex

& calls for automation

Security vulnerabilities are everywhere

& require constant monitoring

Regulatory frameworks are burdensome

& need automated GRC tools

Documentation becomes outdated fast

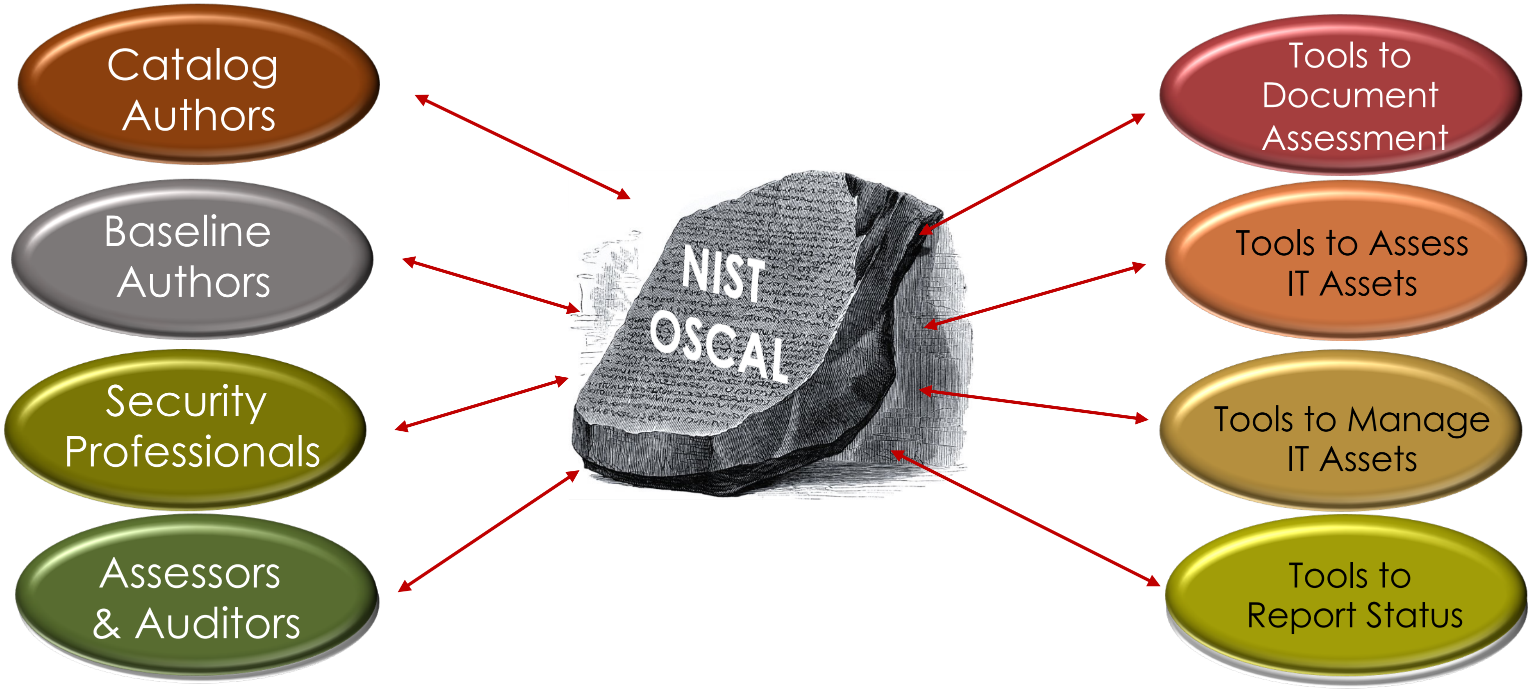
& needs constant updates

Risk management is hard

& experts need help

What is needed? OSCAL!

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

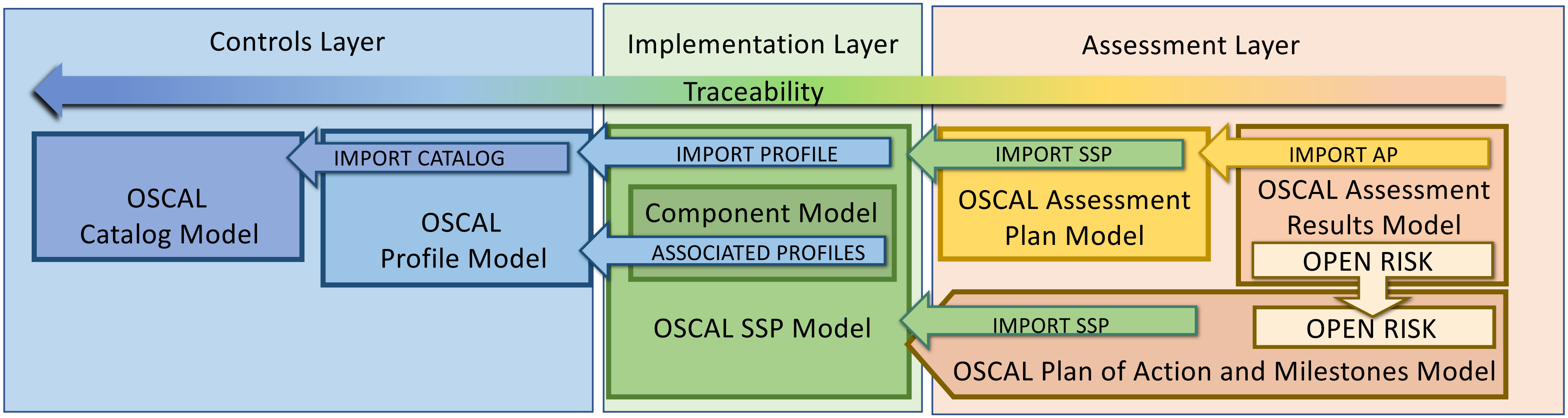


OSCAL sets the foundation for automation and interoperability

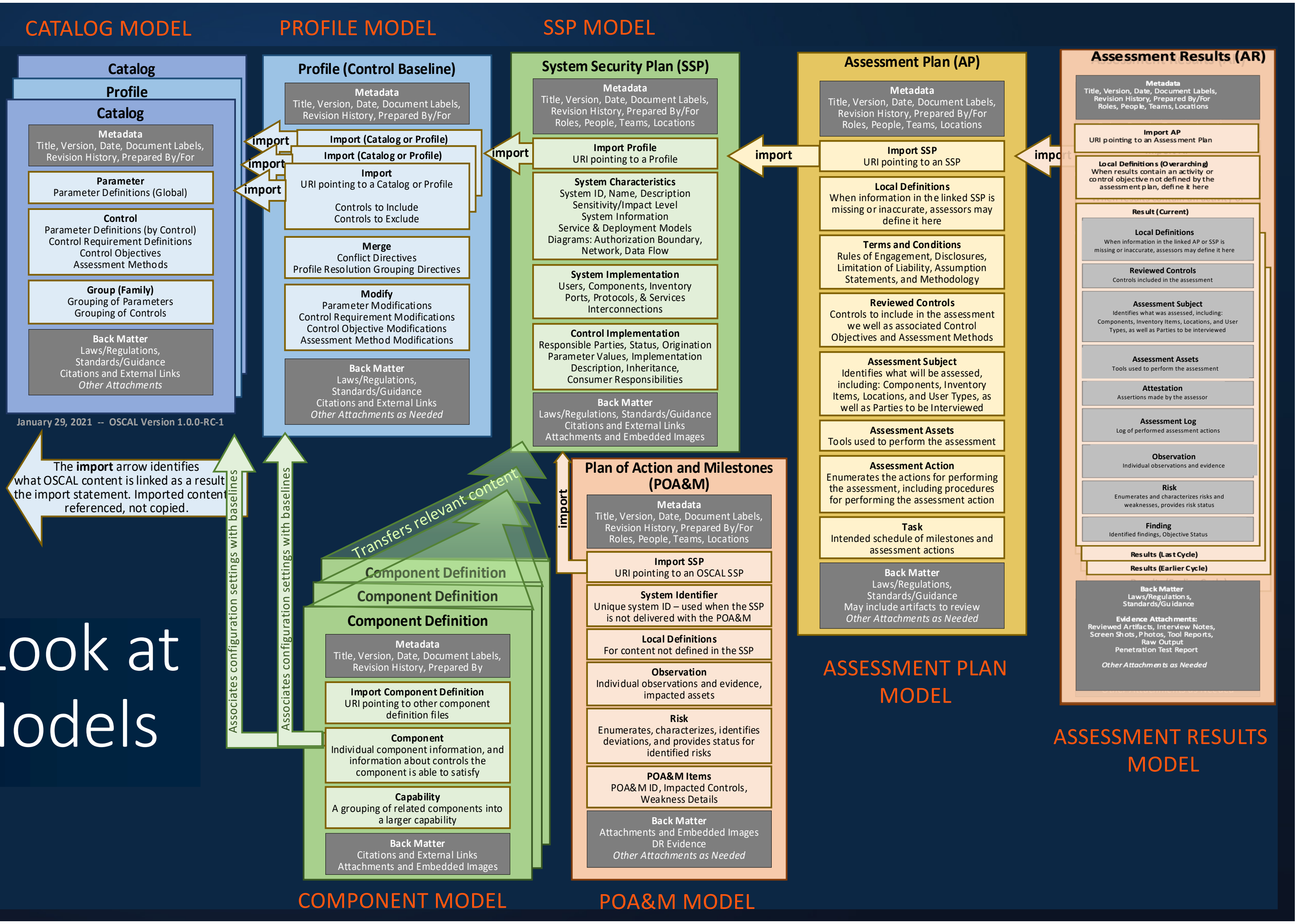
What is OSCAL?

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



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

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

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

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 PLAN 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

ASSESSMENT RESULTS MODEL

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

Associates configuration settings with baselines

Associates configuration settings with baselines

Transfers relevant content

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

COMPONENT MODEL

import

Plan of Action and Milestones (POA&M)

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

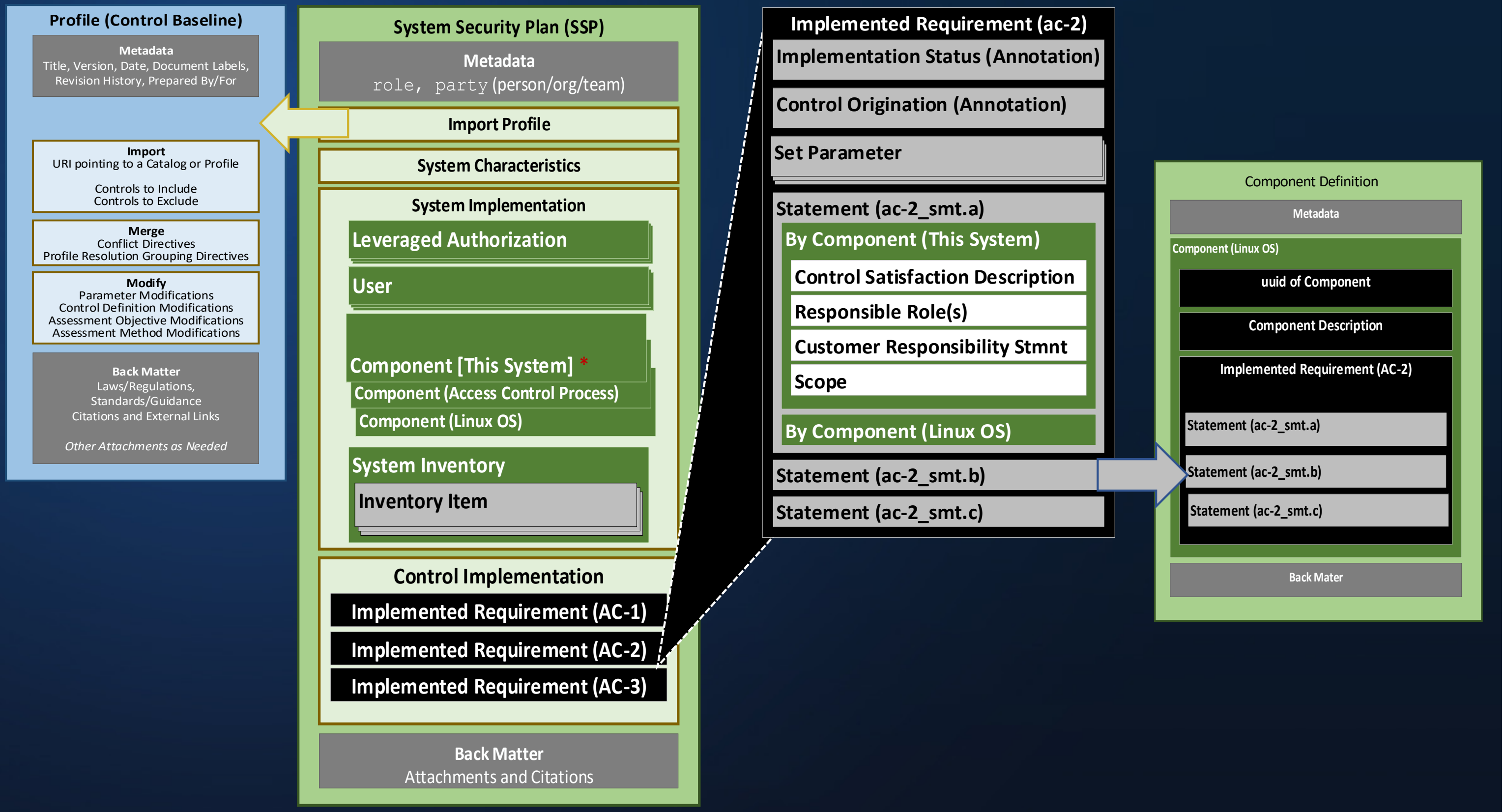
Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

POA&M MODEL

Where the Innovation Truly Starts:
The OSCAL Implementation Layer

OSCAL SSP:

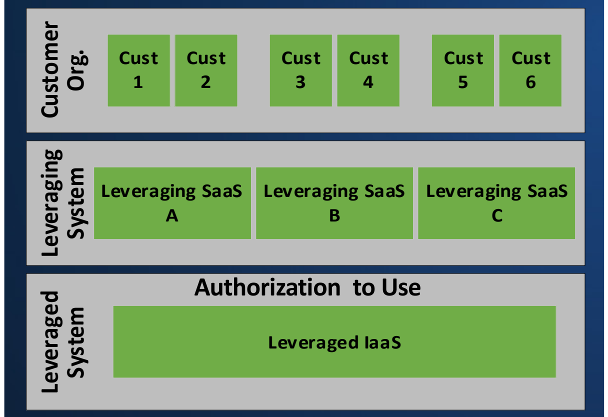
- Imports a Profile identifying the controls
- Each control response is broken down to the individual components involved.
- Enables a more robust response to controls
- Example: The access control implementation that satisfies *AC-2, part a* is described separately for:
  - ❑ This System
  - ❑ The Access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

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

Authorization to Use

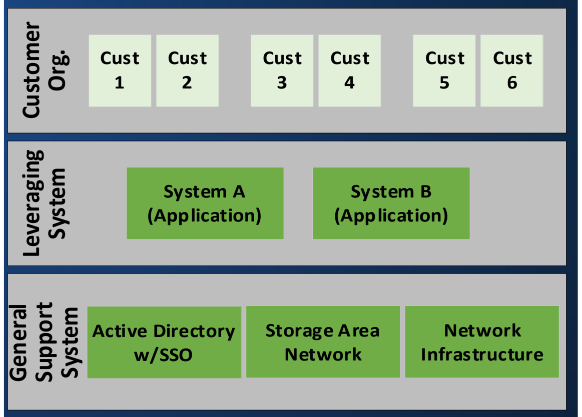
Leveraged System

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)

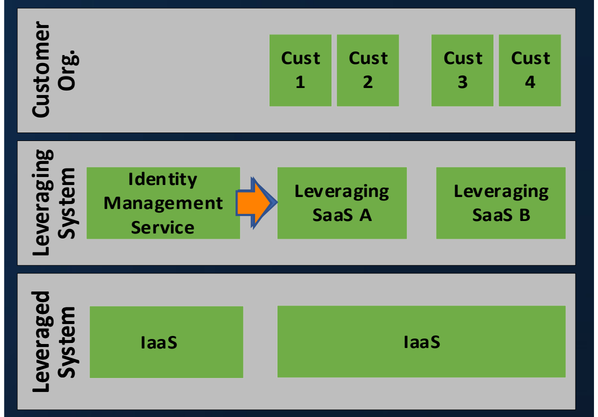
General Support System

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.

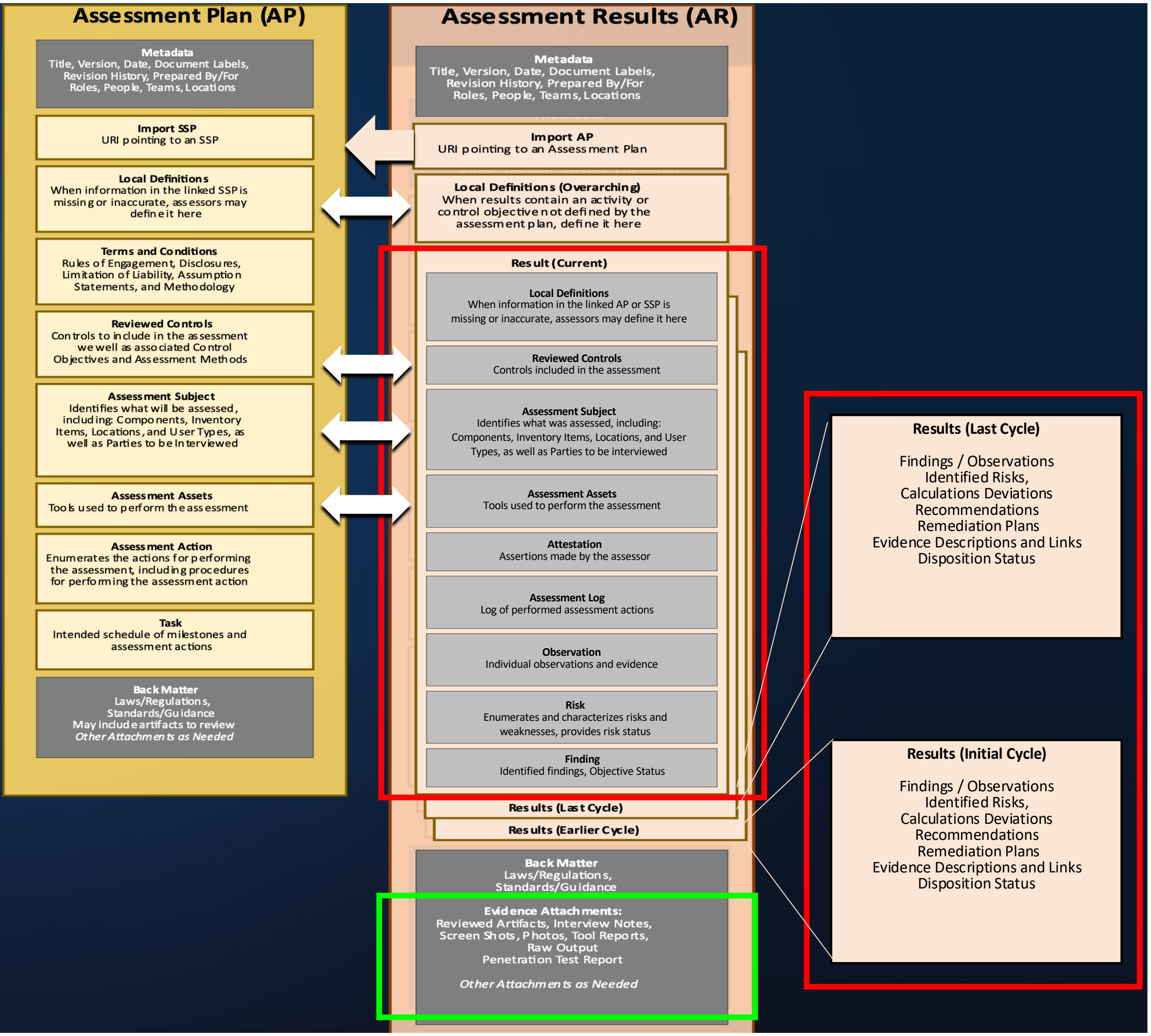
Assessment Plan (SAP) & Assessment Results (AR)

- ➢ 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

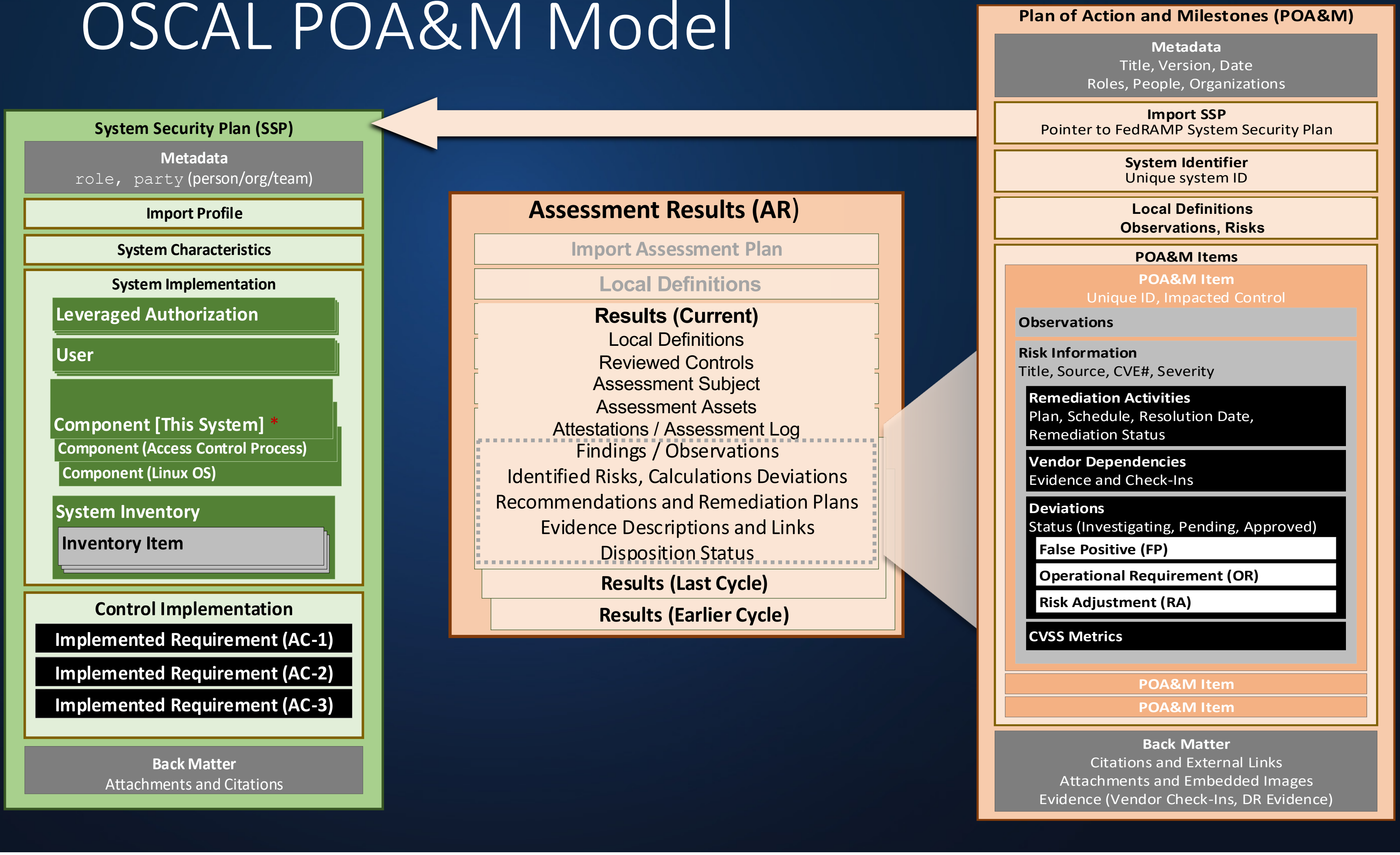
Results (Last Cycle)

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)

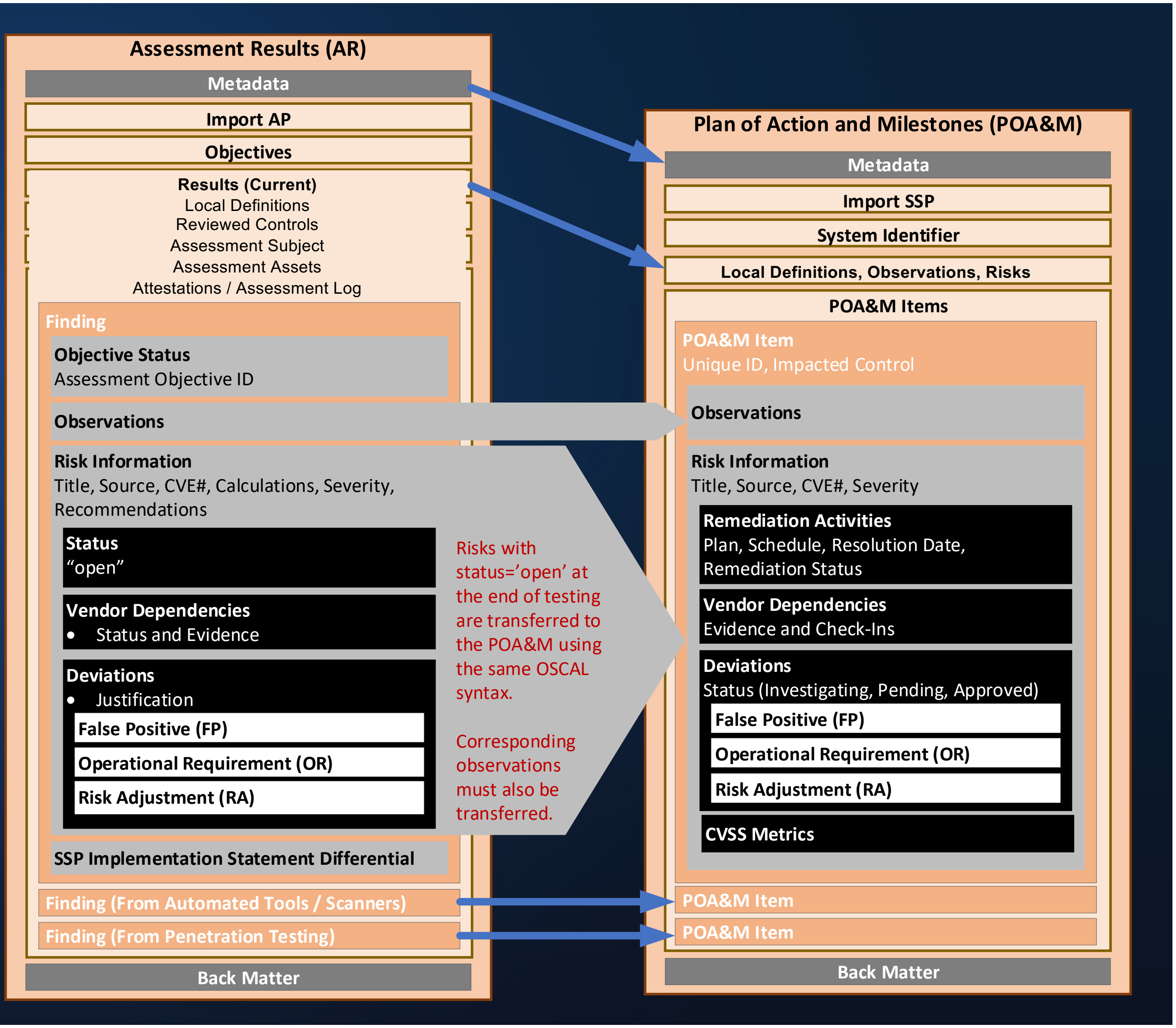
CVSS Metrics

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

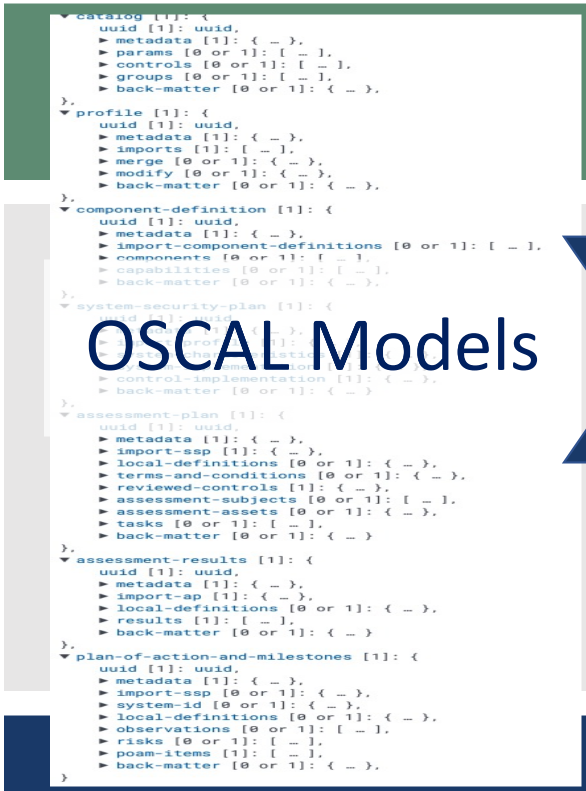
POA&M Item

POA&M Item

Back Matter

Who Can Benefit and How?

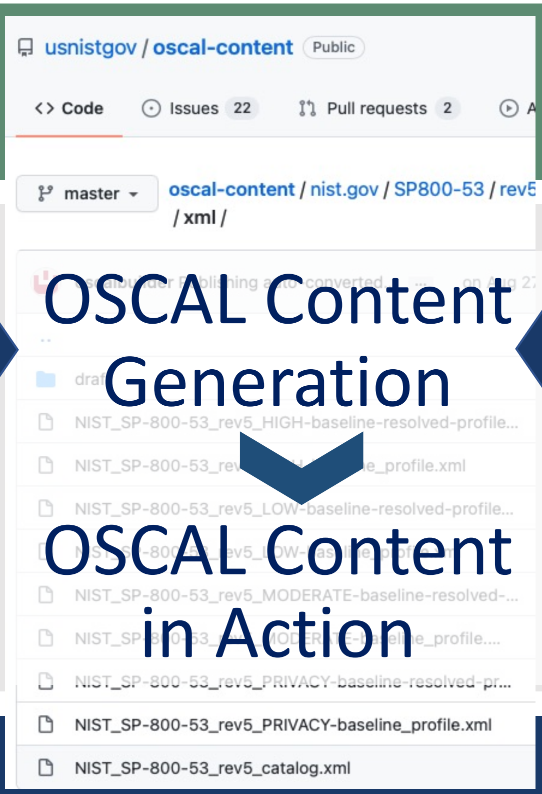
OSCAL Models >>> OSCAL Content >>> OSCAL Tools



```
▼ catalog [1]: {
      uuid [1]: uuid,
    ► metadata [1]: { … },
    ► params [0 or 1]: [ … ],
    ► controls [0 or 1]: [ … ],
    ► groups [0 or 1]: [ … ],
    ► back-matter [0 or 1]: { … },
},
▼ profile [1]: {
      uuid [1]: uuid,
    ► metadata [1]: { … },
    ► imports [1]: [ … ],
    ► merge [0 or 1]: { … },
    ► modify [0 or 1]: { … },
    ► back-matter [0 or 1]: { … },
},
▼ component-definition [1]: {
      uuid [1]: uuid,
    ► metadata [1]: { … },
    ► import-component-definitions [0 or 1]: [ … ],
    ► components [0 or 1]: [ … ],
    ► capabilities [0 or 1]: [ … ],
    ► back-matter [0 or 1]: { … },
},
▼ system-security-plan [1]: {
      uuid [1]: uuid,
    ► metadata [1]: { … },
    ► import-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]: { … },
}
```

OSCAL Models

https://github.com/usnistgov/OSCAL



usnistgov / oscal-content Public

master

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

[illegible] Publishing auto-converted [illegible] on Aug 27

..

draft

NIST_SP-800-53_rev5_HIGH-baseline-resolved-profile...

NIST_SP-800-53_rev5_HIGH-baseline_profile.xml

NIST_SP-800-53_rev5_LOW-baseline-resolved-profile...

NIST_SP-800-53_rev5_LOW-baseline_profile.xml

NIST_SP-800-53_rev5_MODERATE-baseline-resolved-...

NIST_SP-800-53_rev5_MODERATE-baseline_profile....

NIST_SP-800-53_rev5_PRIVACY-baseline-resolved-pr...

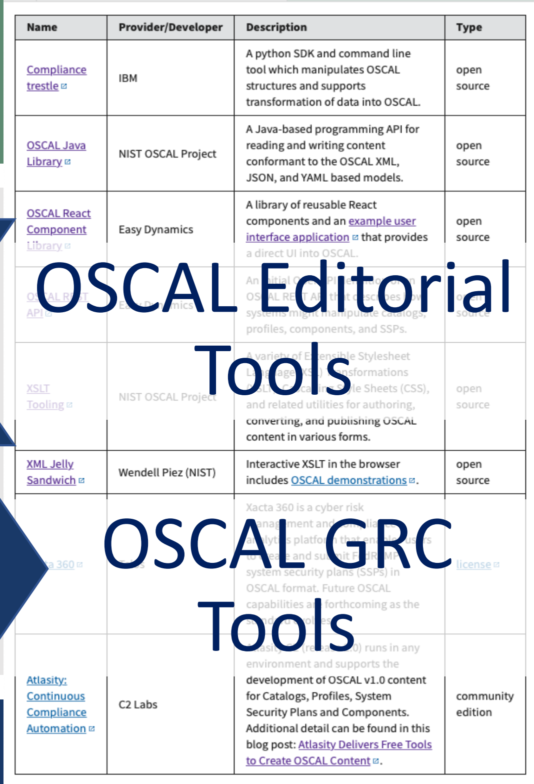
NIST_SP-800-53_rev5_PRIVACY-baseline_profile.xml

NIST_SP-800-53_rev5_catalog.xml

OSCAL Content Generation

OSCAL Content in Action

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



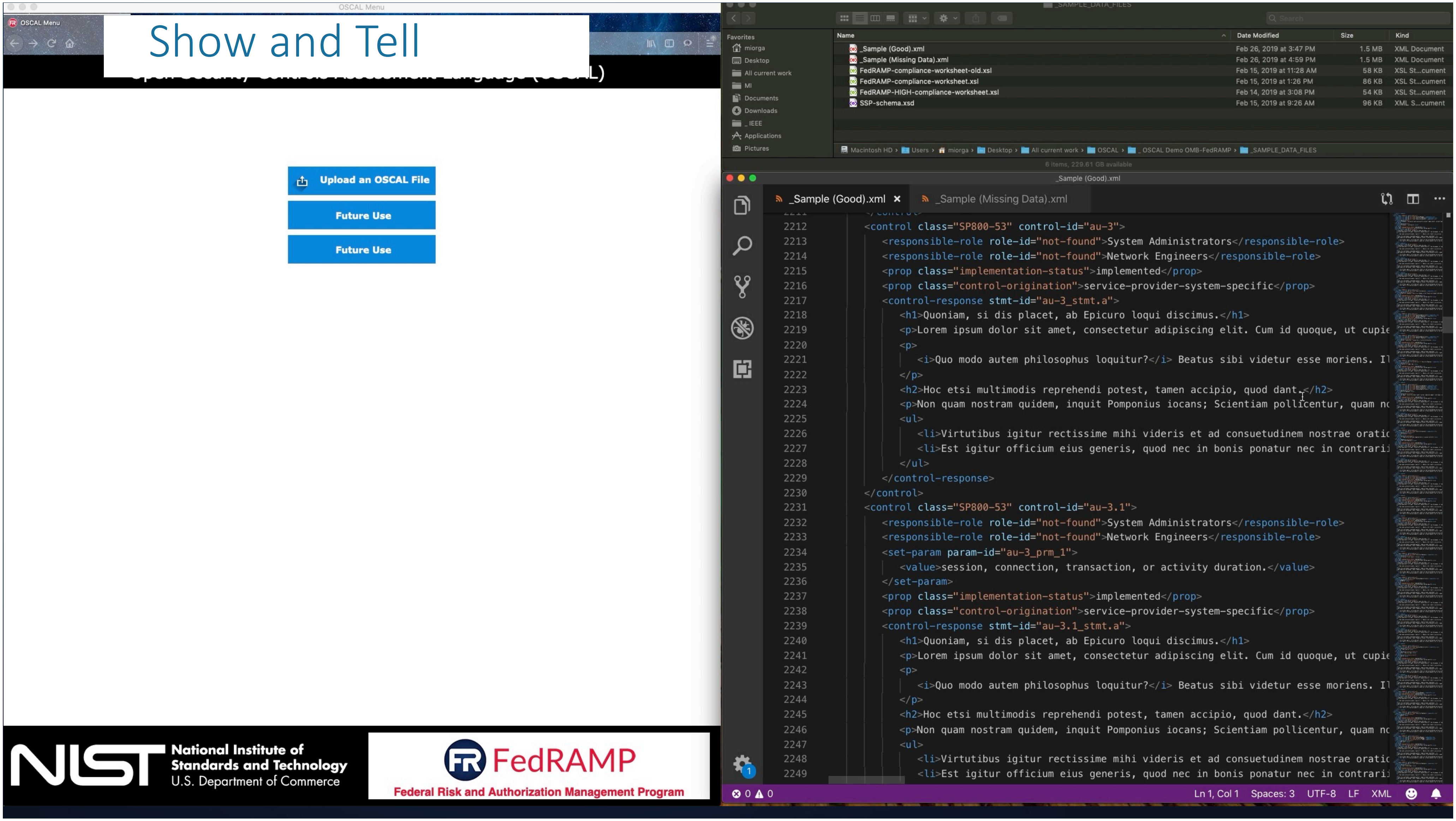
Name	Provider/Developer	Description	Type
Compliance trestle	IBM	A python SDK and command line tool which manipulates OSCAL structures and supports transformation of data into OSCAL.	open source
OSCAL Java Library	NIST OSCAL Project	A Java-based programming API for reading and writing content conformant 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
OSCAL REST API	Easy Dynamics	An initial OpenAPI definition of an OSCAL REST API that describes how systems might manipulate catalogs, profiles, components, and SSPs.	open 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
[illegible]a 360	[illegible]	Xacta 360 is a cyber risk management and compliance analytics platform that enables users to create and submit FedRAMP system security plans (SSPs) in OSCAL format. Future OSCAL capabilities are forthcoming as the standard evolves.	license
Atlasity: Continuous Compliance Automation	C2 Labs	Atlasity CE (release [illegible].0) 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

Show and Tell


OSCAL Menu
Open Security Controls Assessment Language (OSCAL)
Upload an OSCAL File
Future Use
Future Use
National Institute of Standards and Technology
U.S. Department of Commerce
FedRAMP
Federal Risk and Authorization Management Program
_SAMPLE_DATA_FILES
Favorites
miorga
Desktop
All current work
MI
Documents
Downloads
_ IEEE
Applications
Pictures
_Sample (Good).xml
_Sample (Missing Data).xml

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

Macintosh HD › Users › miorga › Desktop › All current work › OSCAL › _ OSCAL Demo OMB-FedRAMP › _SAMPLE_DATA_FILES

6 items, 229.61 GB available

```xml
<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 contrarii
      </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 contrarii
```

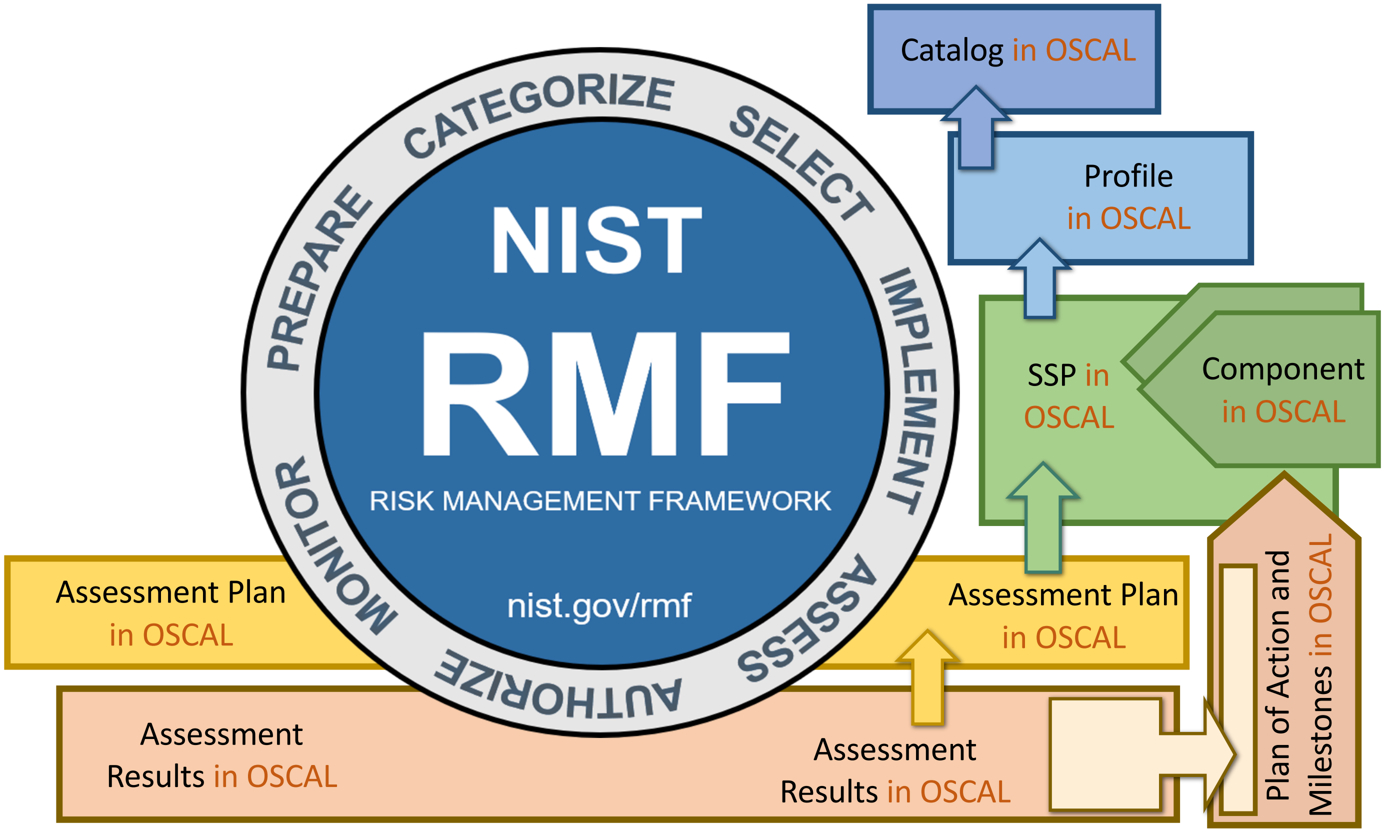
⊗ 0 ⚠ 0 Ln 1, Col 1 Spaces: 3 UTF-8 LF XML

OSCAL Support for Continuously Authorizing Systems to Operate

Authorization to Use
Common Control Authorization

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

OSCAL Content & Risk Management Framework



Security Assessment Automation … with OSCAL

NIST

BASED ON NIST 800-37 rev2

1 System Categorization (OSCAL SSP)

- System Description
- Security Categorization
- Control Selection & Tailoring & Allocation
- Document Control Implementations
- ConMon Planning

2 System & Components Implementation (OSCAL Cdef & SSP)

- Implement Controls and update them
- Document system hardening rules

3 System Assessment (OSCAL AP/AR/POA&M

- Assessor Selection
- Assessment Plan
- Control Assessment
- Assessment Reports (findings & remediations)
- POA&M

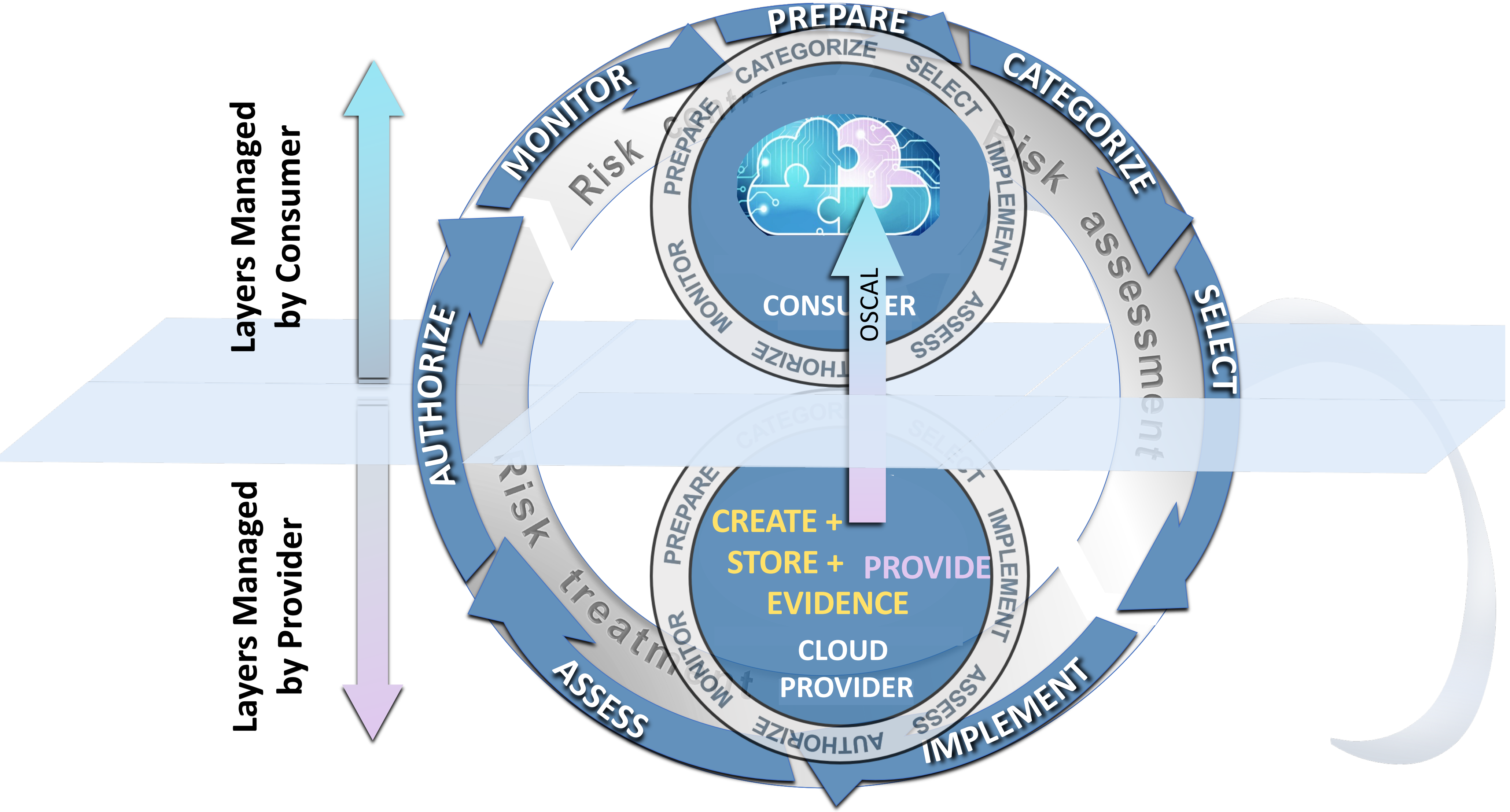
4 System Authorization

- ATO packaging
- Analyze and determine the risk.
- Risk response
- ATO decision
- Ongoing Assessment
- Ongoing risk response

OSCAL Support for Leveraging Authorizations

Authorization to Use
Common Control Authorization

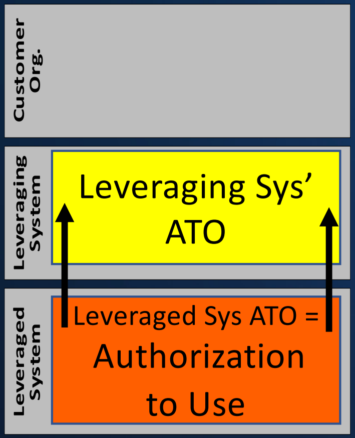
National Institute of Standards and Technology
U.S. Department of Commerce


Layers Managed by Consumer
Layers Managed by Provider
PREPARE
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
Risk
Risk assessment
Risk treatment
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE
CONSUMER
OSCAL
CREATE +
STORE +
PROVIDE
EVIDENCE
CLOUD
PROVIDER

Authorization to Use for a Leveraging System

An Authorization to Use is issued when:

- ○ one or more leveraging systems rely on a system for operation in a stacked hierarchy; and
- ○ an Authorization to Operate was issued to the leveraged system
- ○ any leveraging system is authorized separately from the leveraged system.



Customer Org.

Leveraging System

Leveraging Sys' ATO

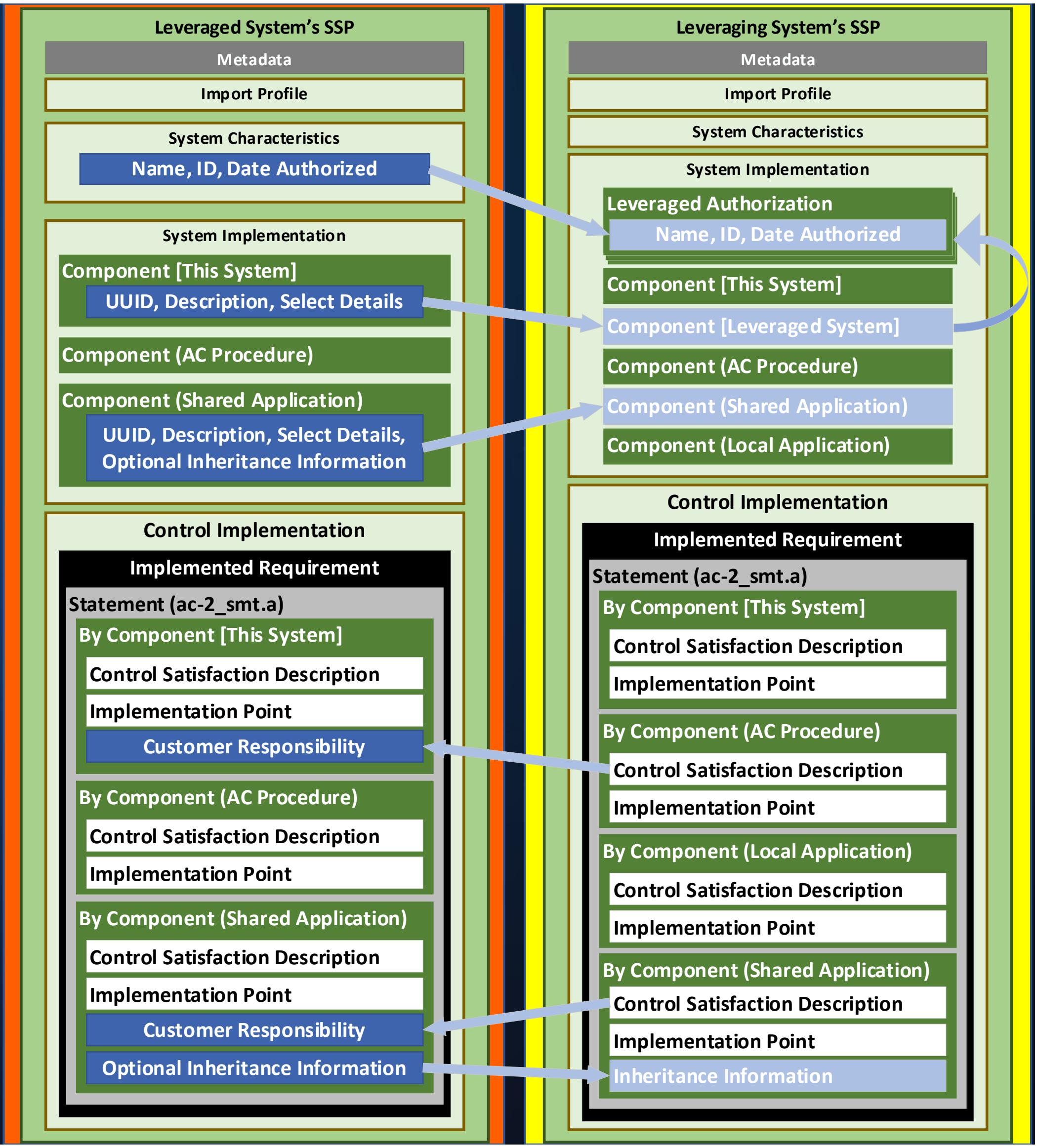
Leveraged System

Leveraged Sys ATO = Authorization to Use

Systems Operating in a Stacked Hierarchy

NOTE:

External services and interconnections are not regarded as leveraged authorizations.



Leveraged System's SSP

Metadata

Import Profile

System Characteristics

Name, ID, Date Authorized

System Implementation

Component [This System]

UUID, Description, Select Details

Component (AC Procedure)

Component (Shared Application)

UUID, Description, Select Details, Optional Inheritance Information

Control Implementation

Implemented Requirement

Statement (ac-2_smt.a)

By Component [This System]

Control Satisfaction Description

Implementation Point

Customer Responsibility

By Component (AC Procedure)

Control Satisfaction Description

Implementation Point

By Component (Shared Application)

Control Satisfaction Description

Implementation Point

Customer Responsibility

Optional Inheritance Information

Leveraging System's SSP

Metadata

Import Profile

System Characteristics

System Implementation

Leveraged Authorization

Name, ID, Date Authorized

Component [This System]

Component [Leveraged System]

Component (AC Procedure)

Component (Shared Application)

Component (Local Application)

Control Implementation

Implemented Requirement

Statement (ac-2_smt.a)

By Component [This System]

Control Satisfaction Description

Implementation Point

By Component (AC Procedure)

Control Satisfaction Description

Implementation Point

By Component (Local Application)

Control Satisfaction Description

Implementation Point

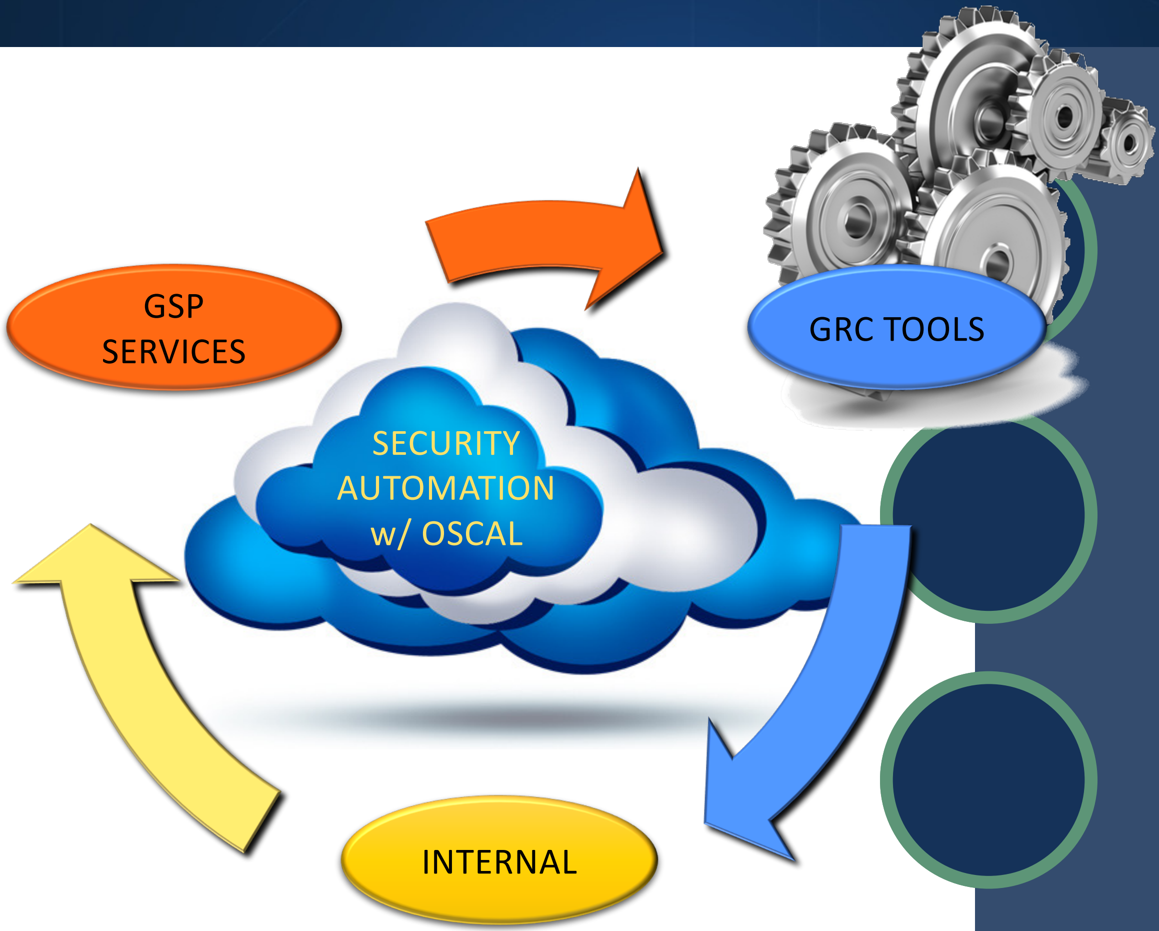
By Component (Shared Application)

Control Satisfaction Description

Implementation Point

Inheritance Information

OSCAL-BASED AUTOMATION



INTERNAL SECURITY/COMPLIANCE TEAMS:

- create/store/provide evidence

GCP SERVICES :

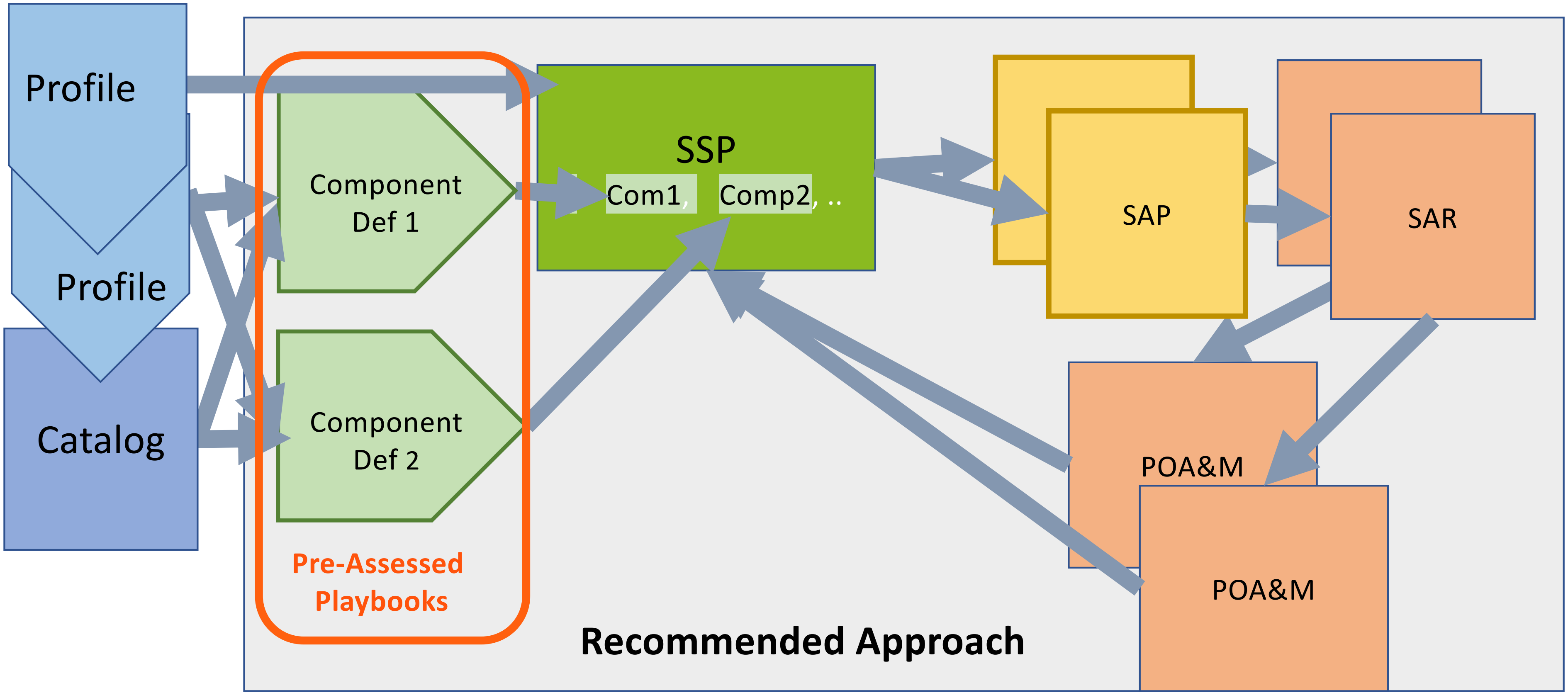
- continuous compliance attestation/evidence
- document shared security responsibilities

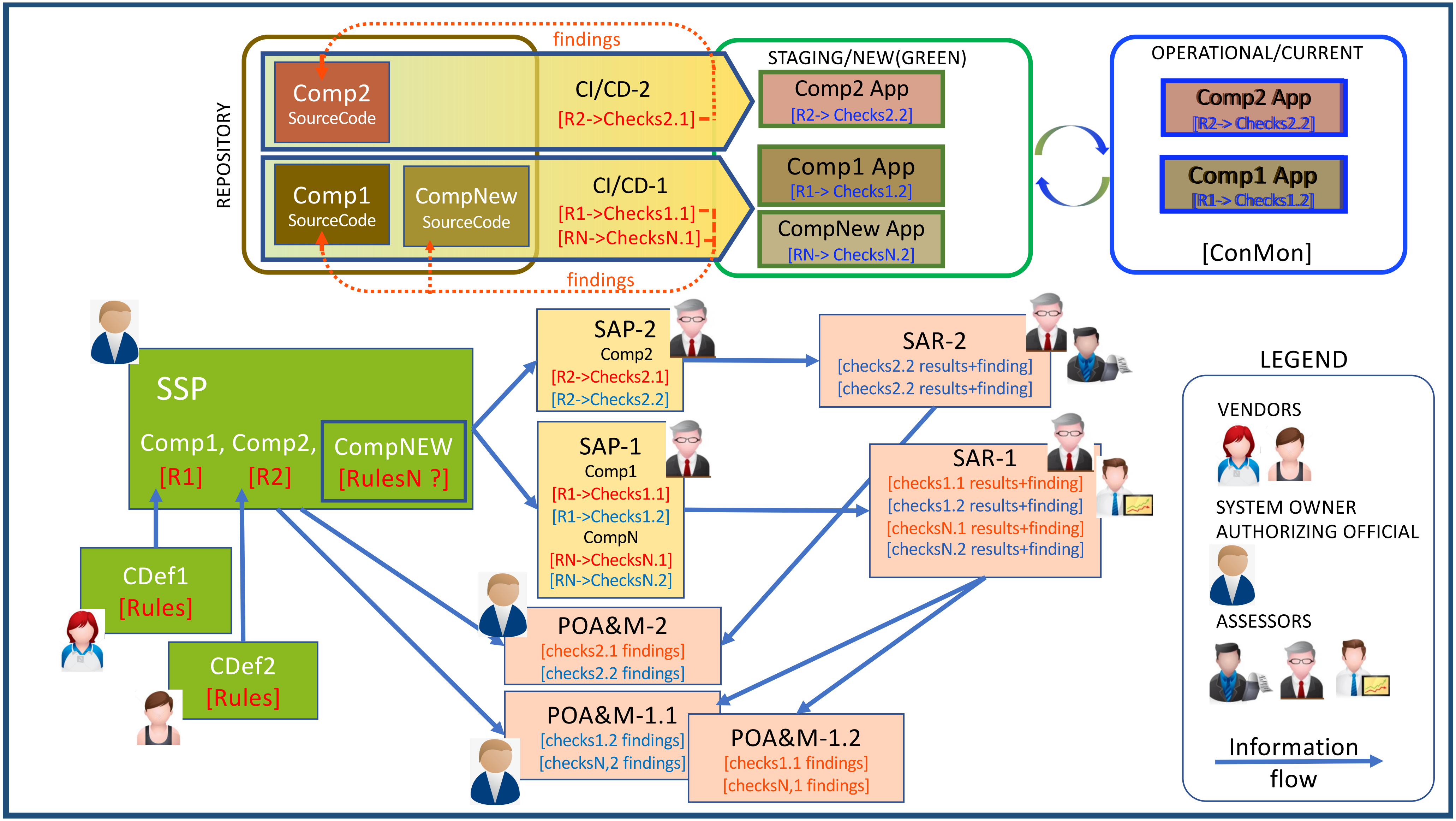
GRC TOOLS DEVELOPMENT OR INTEGRATION

Shifting Left with OSCAL

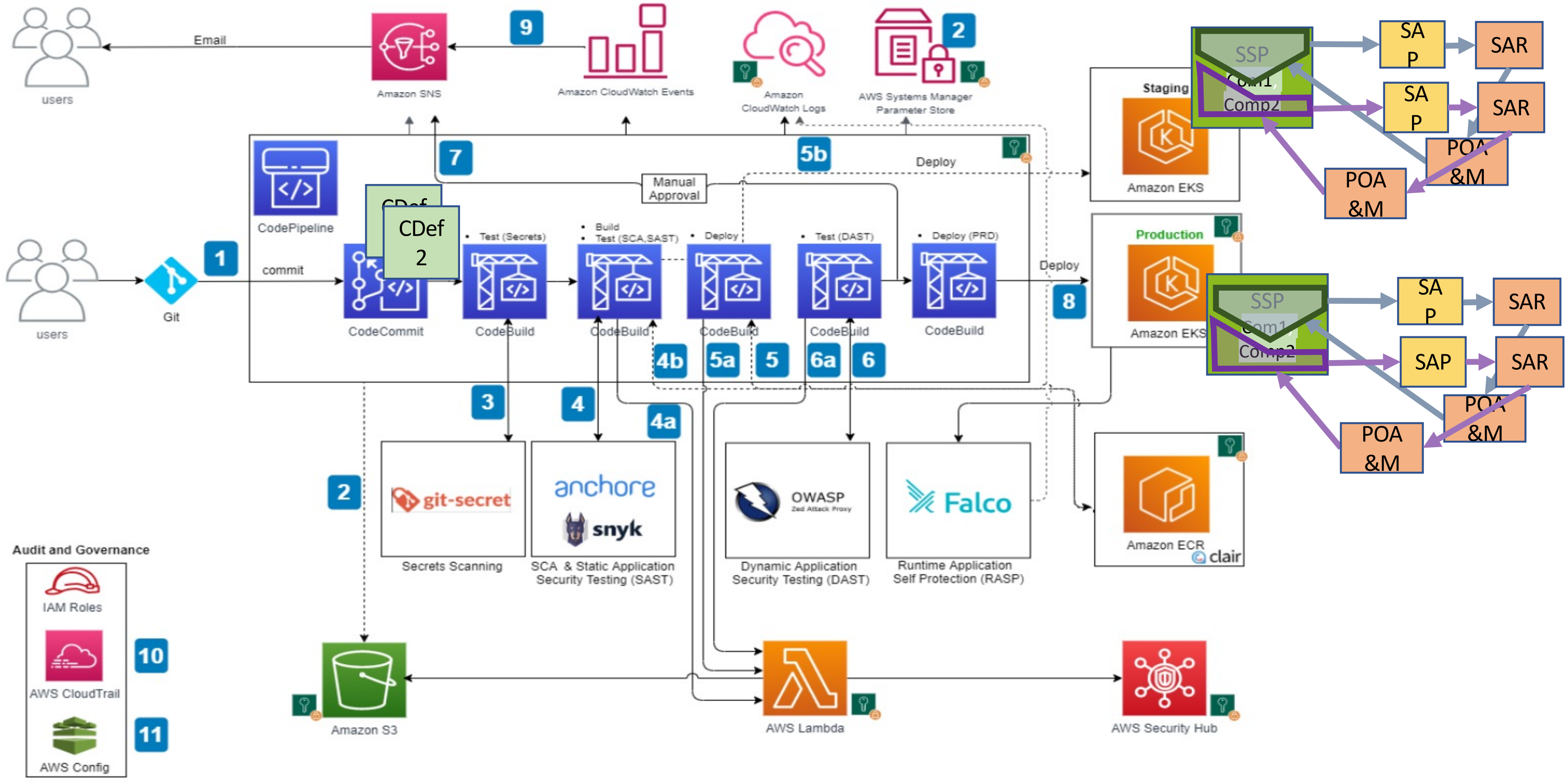
National Institute of Standards and Technology
U.S. Department of Commerce

Shifting Left & Continuous ATO



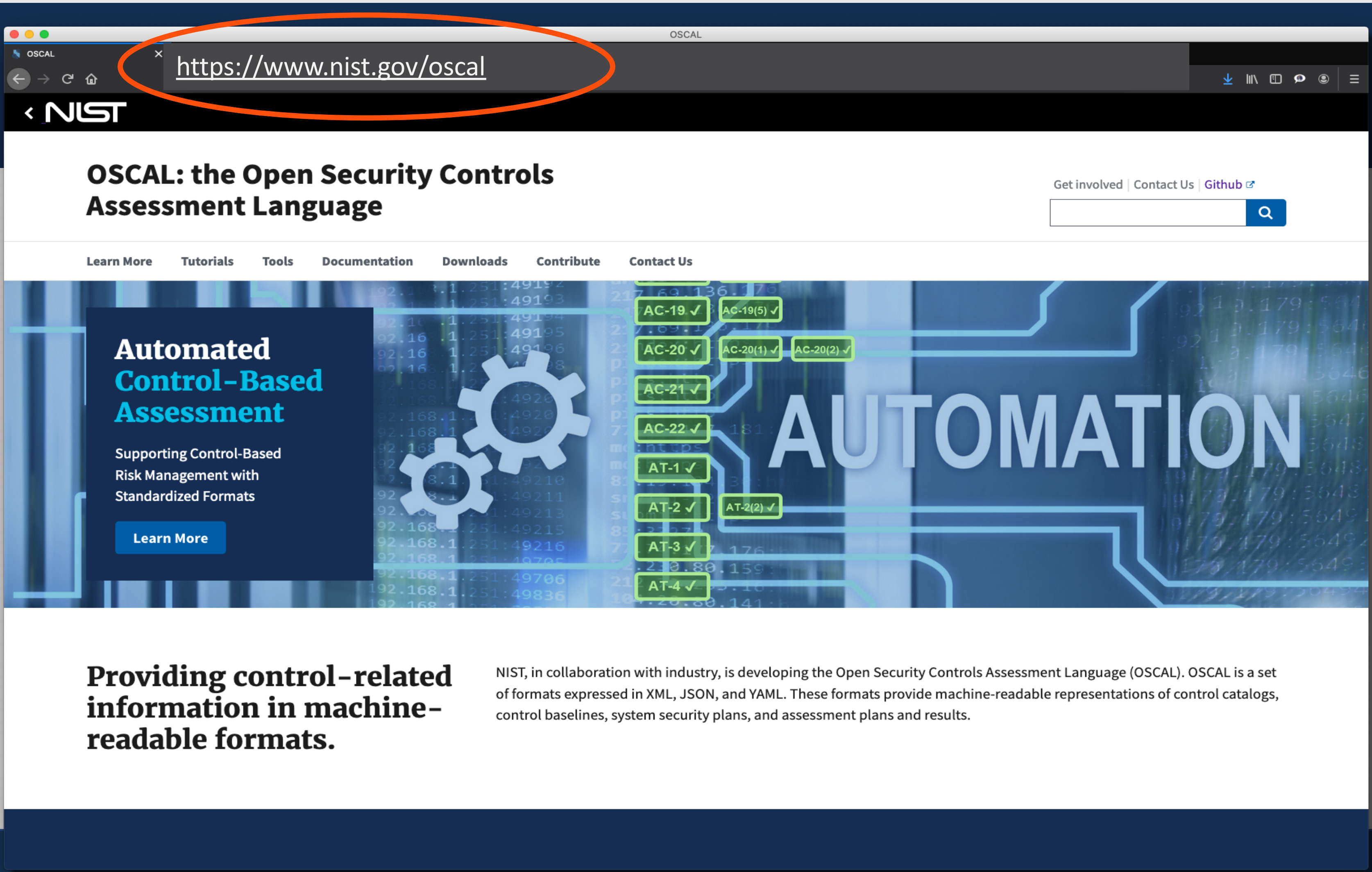

REPOSITORY
findings
Comp2
SourceCode
CI/CD-2
[R2->Checks2.1]
Comp1
SourceCode
CompNew
SourceCode
CI/CD-1
[R1->Checks1.1]
[RN->ChecksN.1]
findings
STAGING/NEW(GREEN)
Comp2 App
[R2-> Checks2.2]
Comp1 App
[R1-> Checks1.2]
CompNew App
[RN-> ChecksN.2]
OPERATIONAL/CURRENT
Comp2 App
[R2-> Checks2.2]
Comp1 App
[R1-> Checks1.2]
[ConMon]
SSP
Comp1, Comp2,
[R1]
[R2]
CompNEW
[RulesN ?]
CDef1
[Rules]
CDef2
[Rules]
SAP-2
Comp2
[R2->Checks2.1]
[R2->Checks2.2]
SAP-1
Comp1
[R1->Checks1.1]
[R1->Checks1.2]
CompN
[RN->ChecksN.1]
[RN->ChecksN.2]
SAR-2
[checks2.2 results+finding]
[checks2.2 results+finding]
SAR-1
[checks1.1 results+finding]
[checks1.2 results+finding]
[checksN.1 results+finding]
[checksN.2 results+finding]
POA&M-2
[checks2.1 findings]
[checks2.2 findings]
POA&M-1.1
[checks1.2 findings]
[checksN,2 findings]
POA&M-1.2
[checks1.1 findings]
[checksN,1 findings]
LEGEND
VENDORS
SYSTEM OWNER
AUTHORIZING OFFICIAL
ASSESSORS
Information
flow

AWS’ Kubernetes DevSecOps Pipeline Architecture



Kubernetes DevSecOps Pipeline Architecture

Courtesy of AWS: https://aws.amazon.com/blogs/devops/building-an-end-to-end-kubernetes-based-devsecops-software-factory-on-aws/



https://www.nist.gov/oscal

OSCAL: the Open Security Controls Assessment Language

Automated Control-Based Assessment

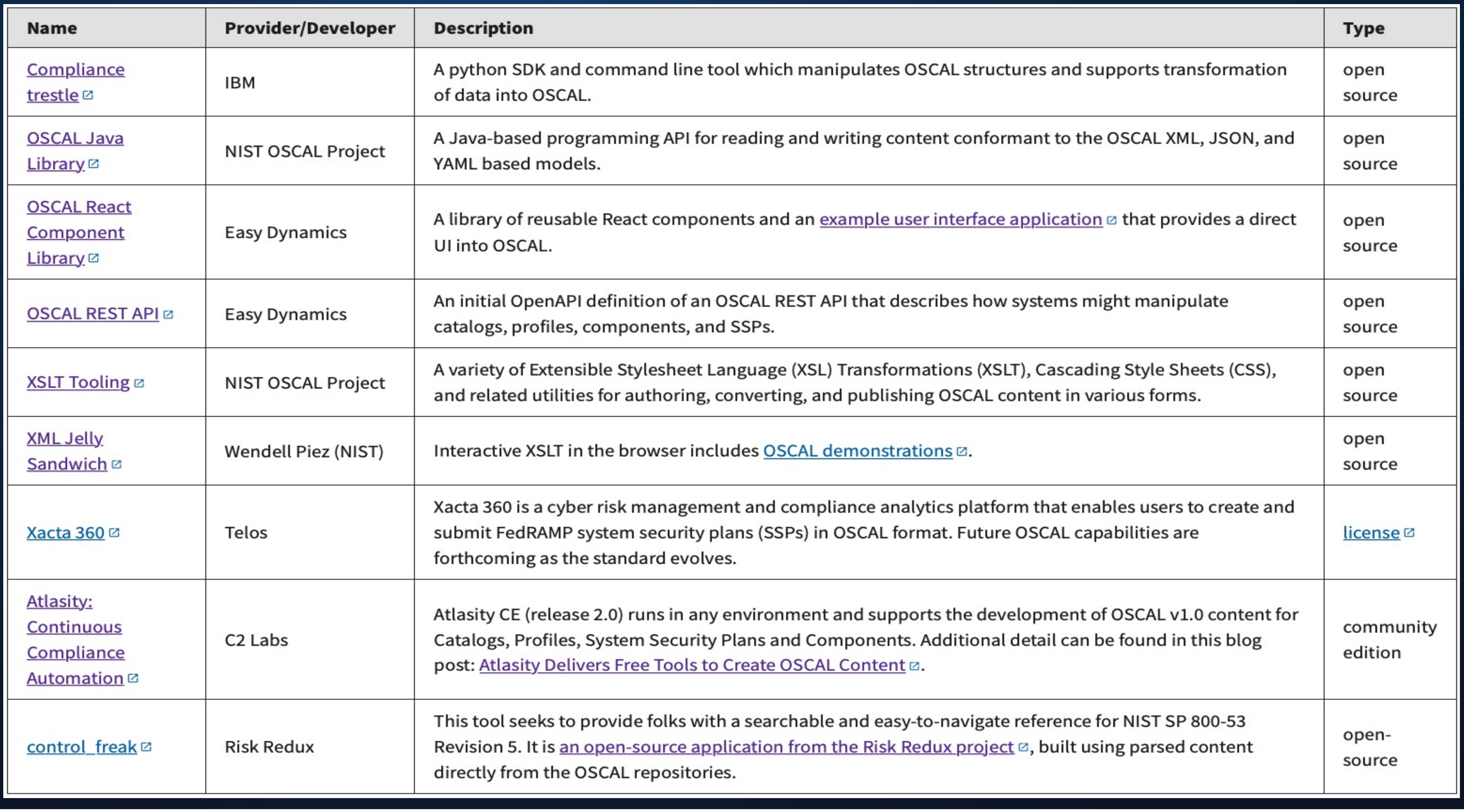
Supporting Control-Based Risk Management with Standardized Formats

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.

Open-Source Tools and Libraries

https://pages.nist.gov/OSCAL/tools/#open-source-tools-and-libraries



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
OSCAL REST API	Easy Dynamics	An initial OpenAPI definition of an OSCAL REST API that describes how systems might manipulate catalogs, profiles, components, and SSPs.	open 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	Telos	Xacta 360 is a cyber risk management and compliance analytics platform that enables users to create and submit FedRAMP system security plans (SSPs) in OSCAL format. Future OSCAL capabilities are forthcoming as the standard evolves.	license
Atlasity: Continuous Compliance Automation	C2 Labs	Atlasity CE (release 2.0) 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
control_freak	Risk Redux	This tool seeks to provide folks with a searchable and easy-to-navigate reference for NIST SP 800-53 Revision 5. It is an open-source application from the Risk Redux project, built using parsed content directly from the OSCAL repositories.	open-source

Few of the 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
- □ KPMG
- □ IBM Research

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

Booz | Allen | Hamilton®

aws

KRATOS®
READY FOR WHAT'S NEXT™

salesforce

ORACLE

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 Community's:
OSCAL Club/awesome-oscal:
https://github.com/oscal-club/awesome-oscal

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

Thank you!