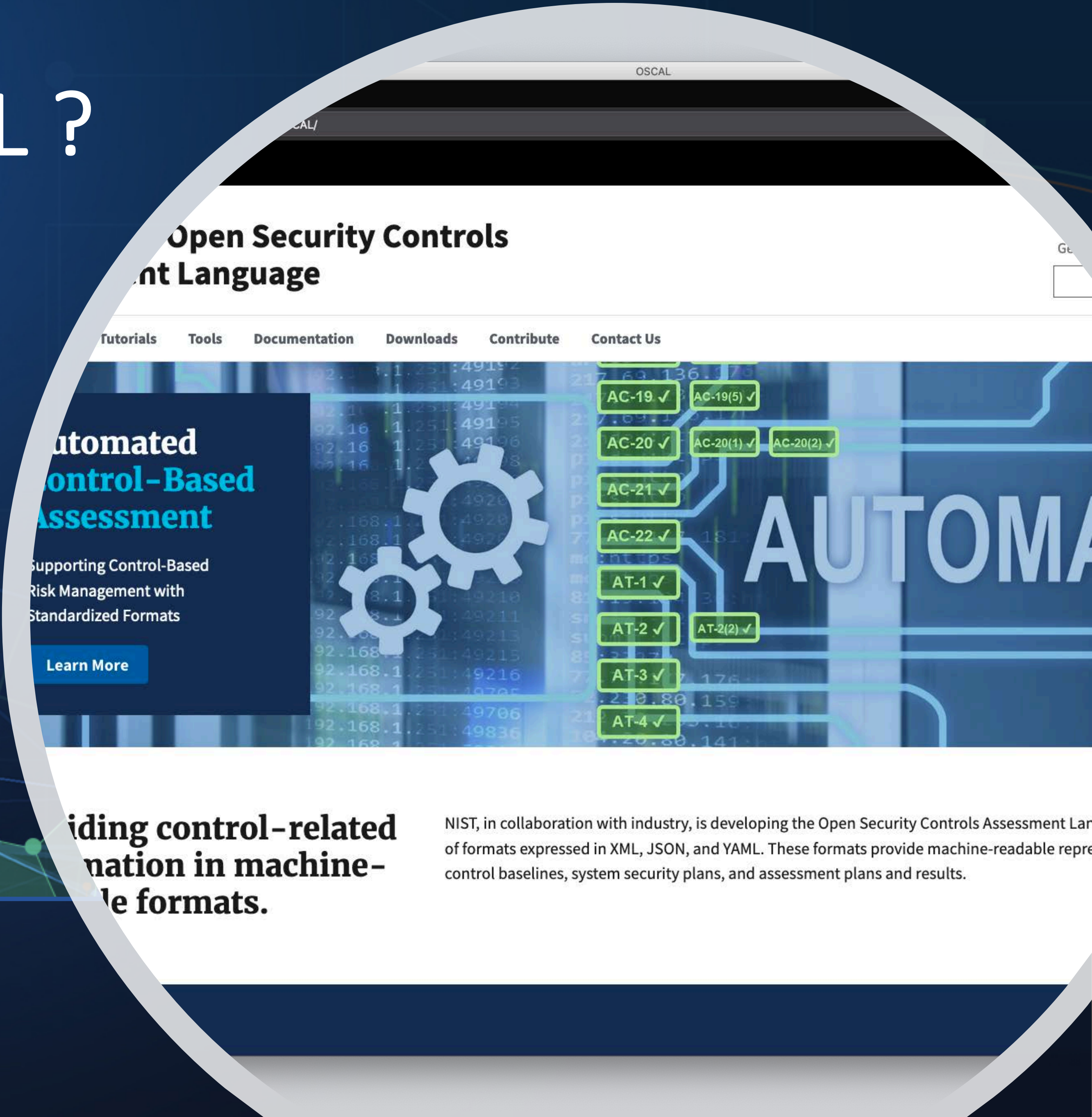
What is OSCAL ?
&
Who Needs It?

February 2, 2021



Open Security Controls
nt Language

utomated
ontrol-Based
ssessment

upporting Control-Based
isk Management with
tandardized Formats

iding control-related
mation in machine-
le formats.

NIST, in collaboration with industry, is developing the Open Security Controls Assessment Lar
of formats expressed in XML, JSON, and YAML. These formats provide machine-readable repre
control baselines, system security plans, and assessment plans and results.

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

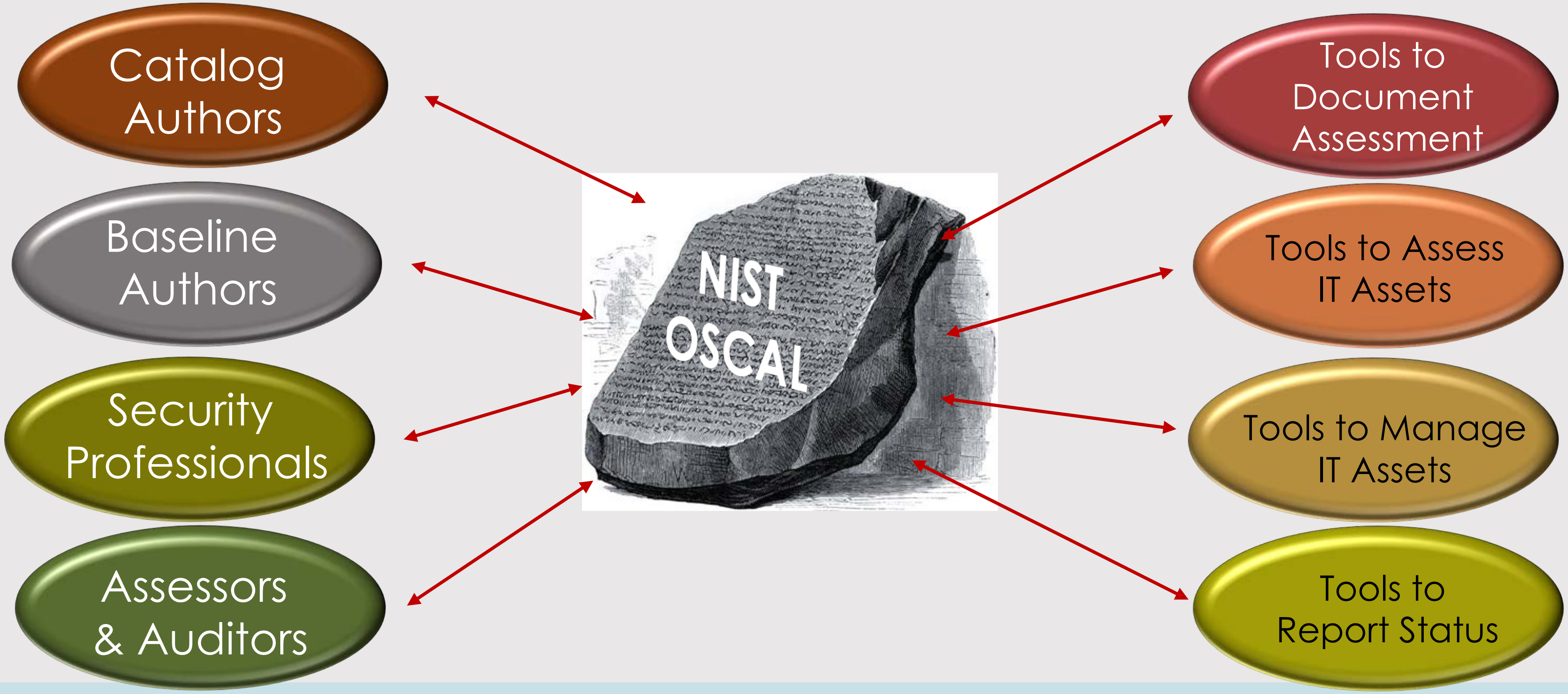
Why we care?

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- Documentatio n becomes outdated fast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 is needed?

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

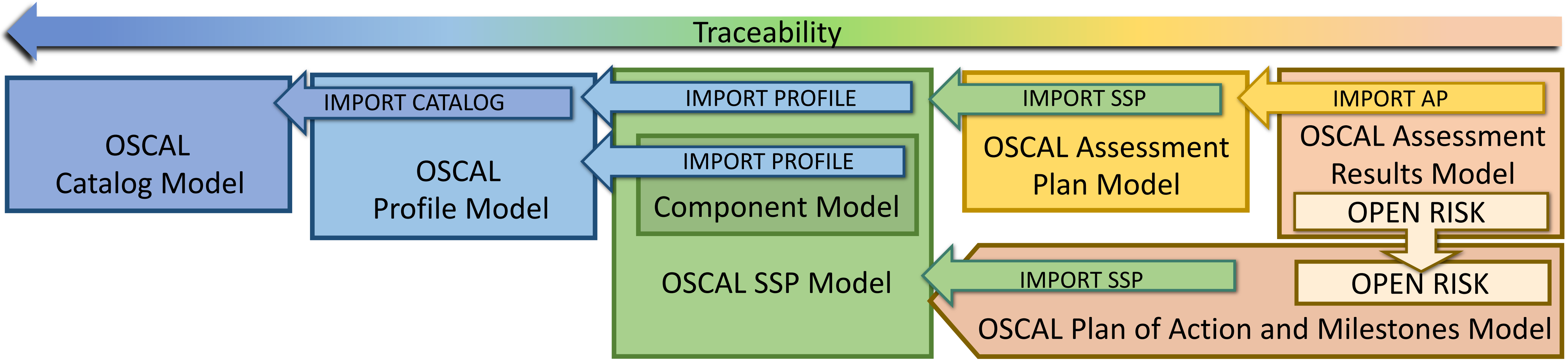


OSCAL sets the foundation for automation and interoperability

What is OSCAL?

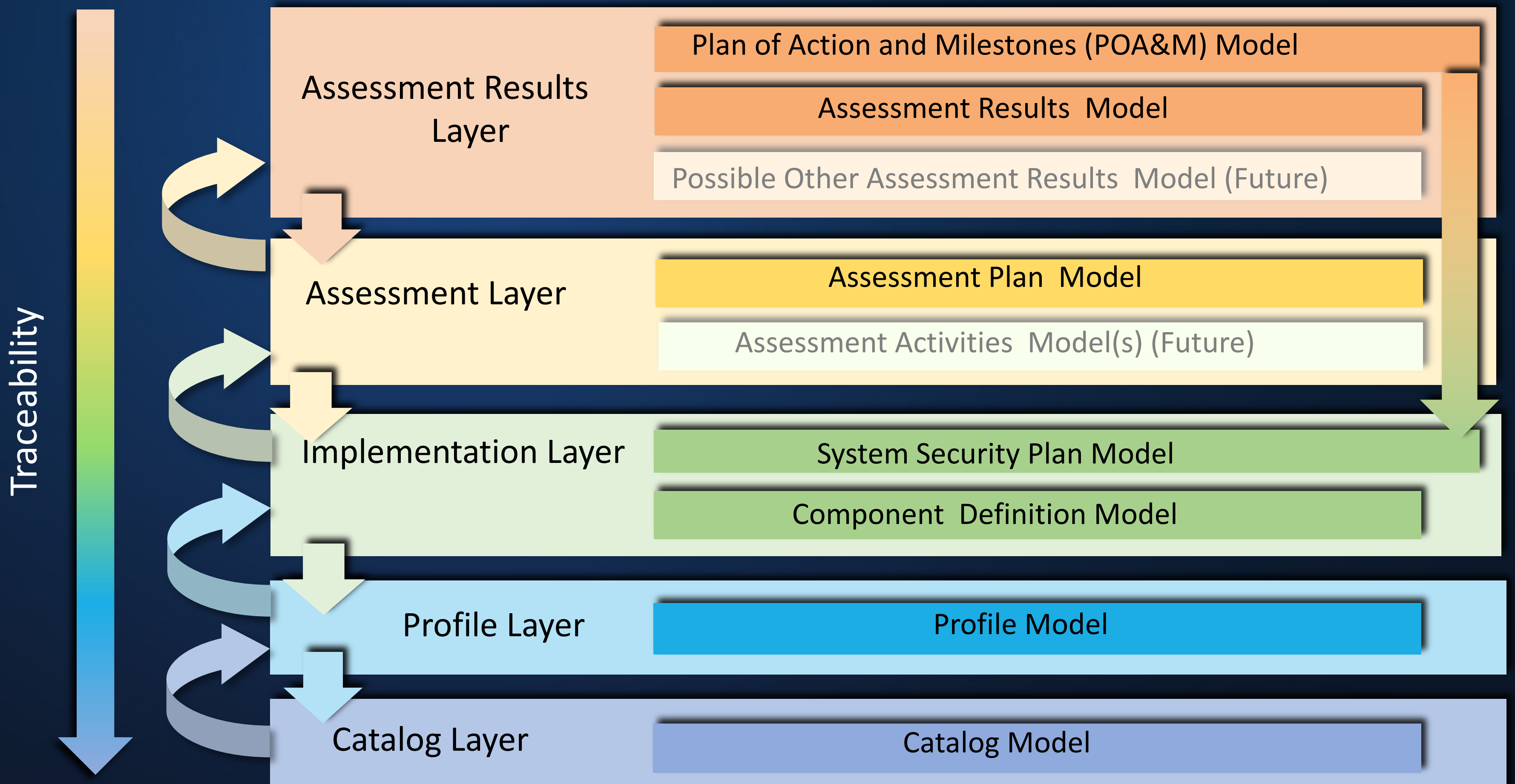
OSCAL is the result of NIST and FedRAMP collaboration

- **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



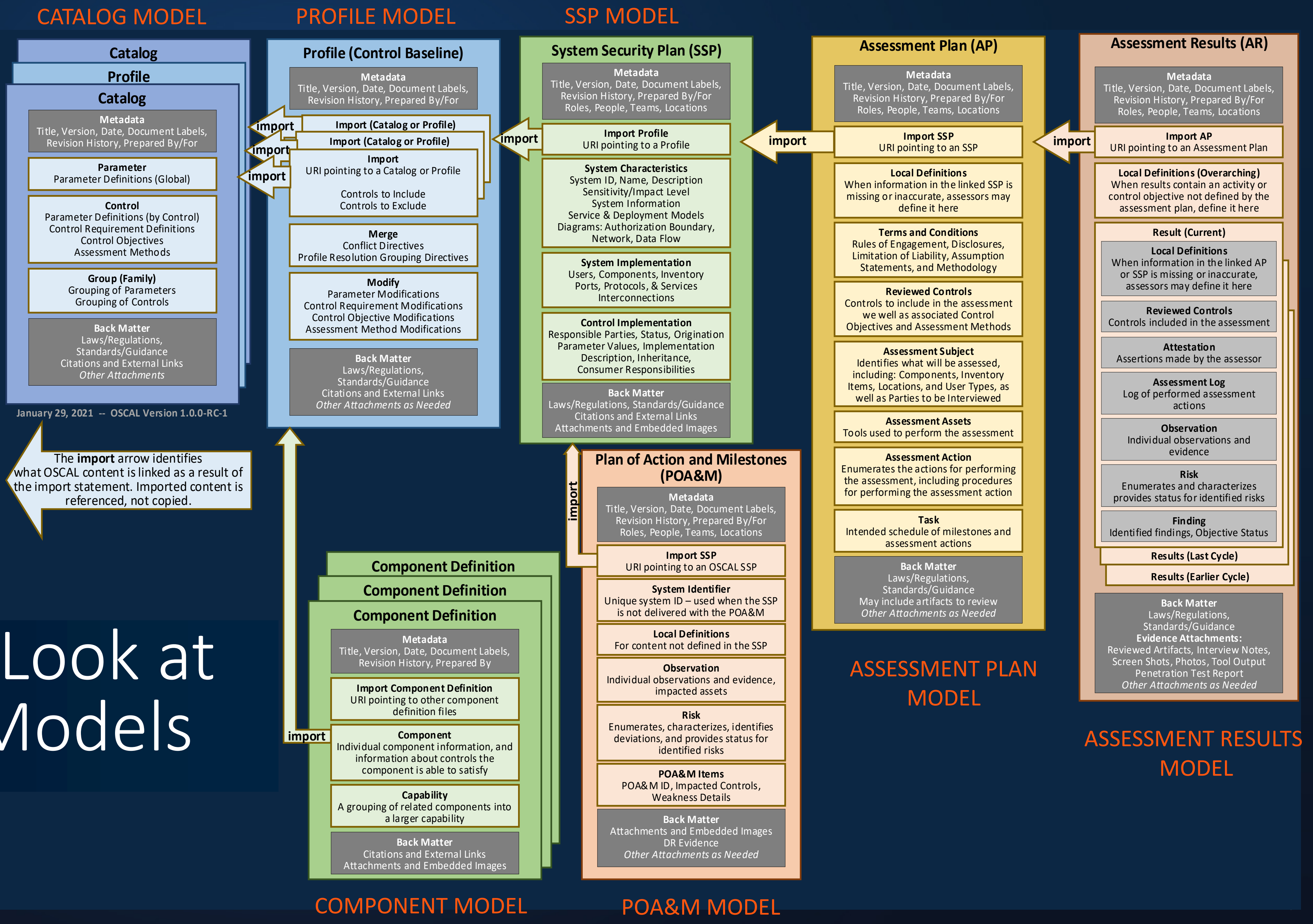
OSCAL Architecture

Layers & Models, v1.0.0. – Release Candidates



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 of the import statement. Imported content is 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

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 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

Attestation
Assertions made by the assessor

Assessment Log
Log of performed assessment actions

Observation
Individual observations and evidence

Risk
Enumerates and characterizes provides status for identified risks

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 Output
Penetration Test Report
Other Attachments as Needed

COMPONENT MODEL

Component Definition

Component Definition

Component Definition

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

import

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)

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

import

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

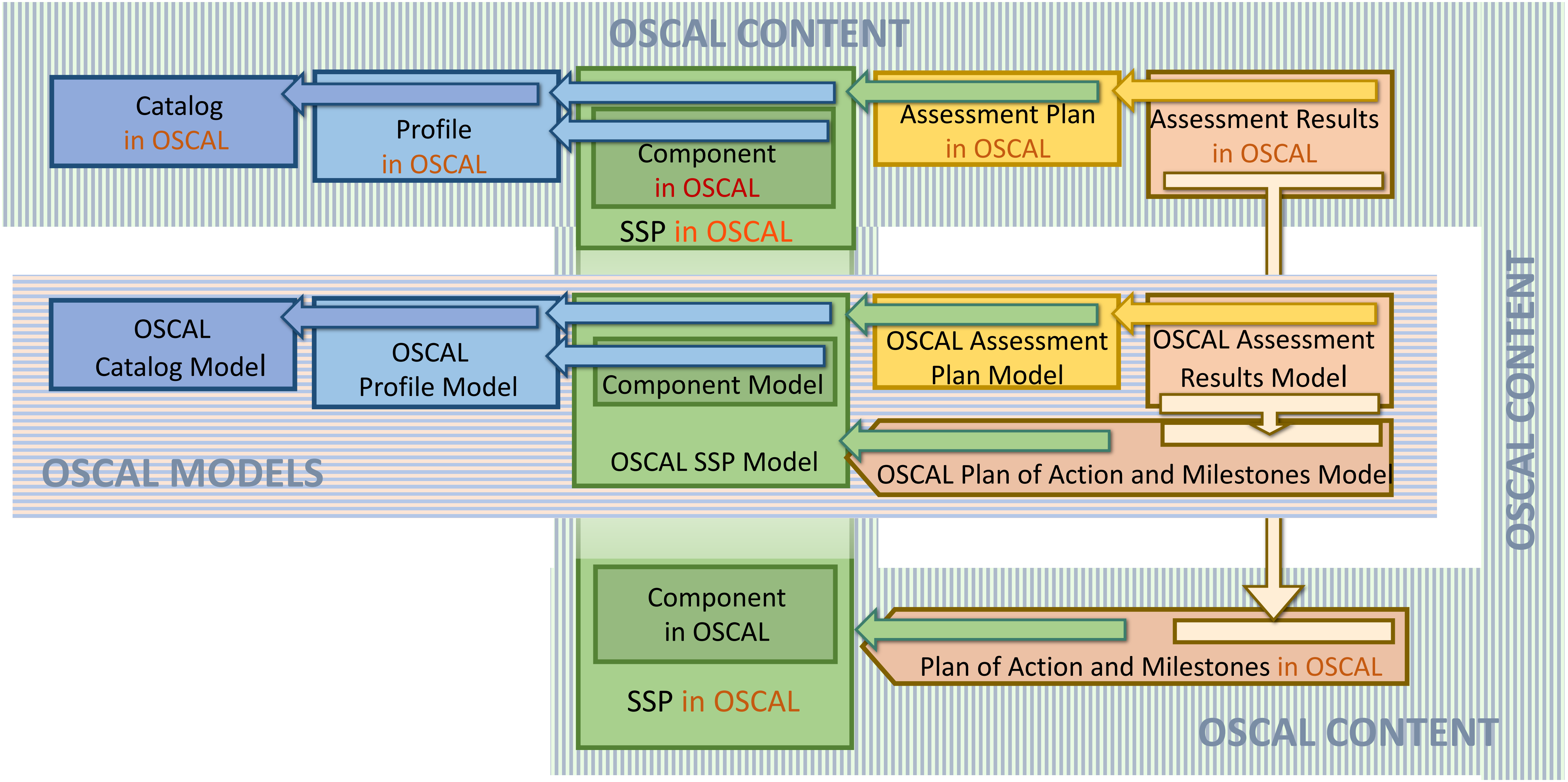
Observation
Individual observations and evidence, impacted assets

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

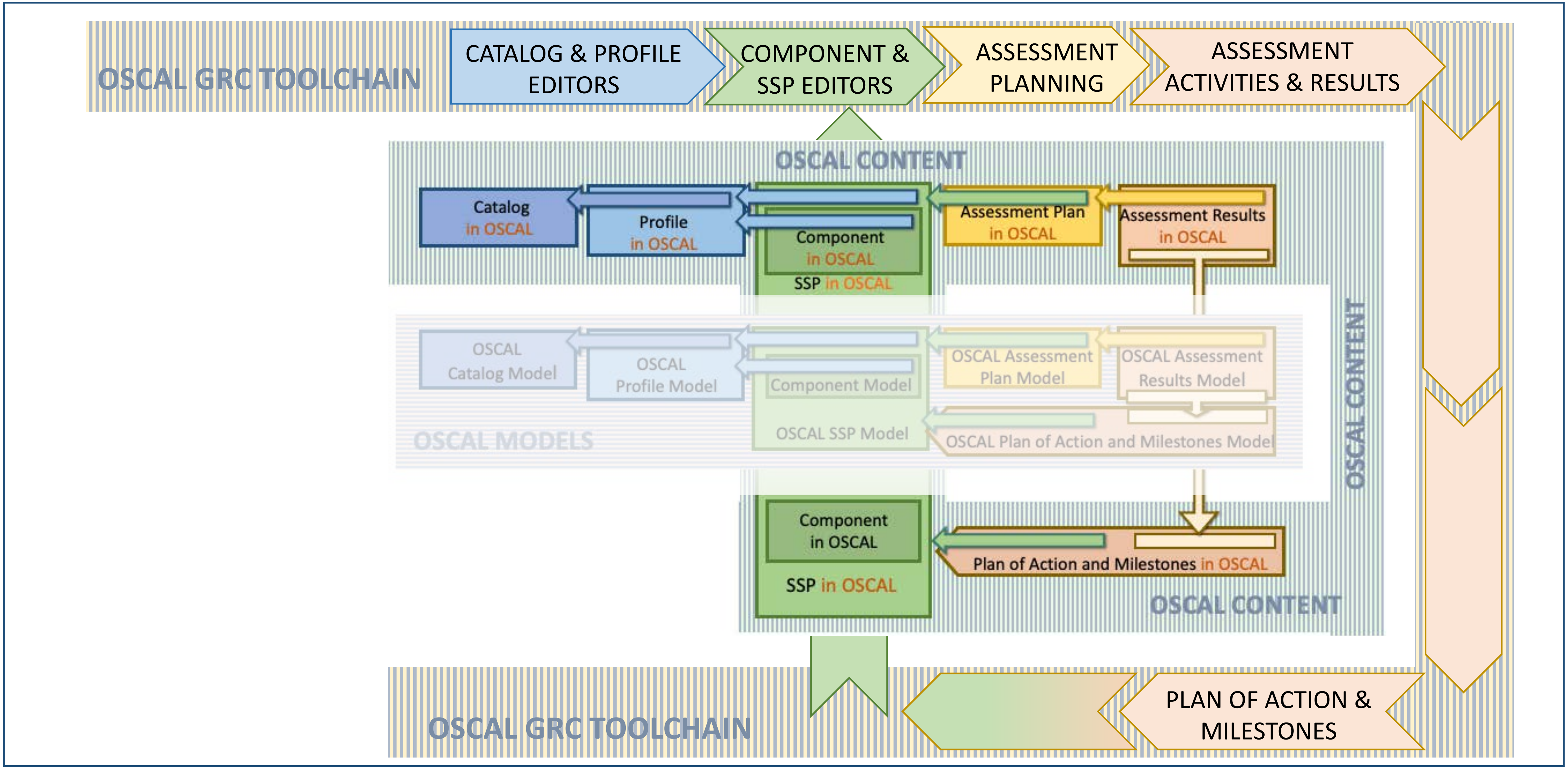
POA&M Items
POA&M ID, Impacted Controls, Weakness Details

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

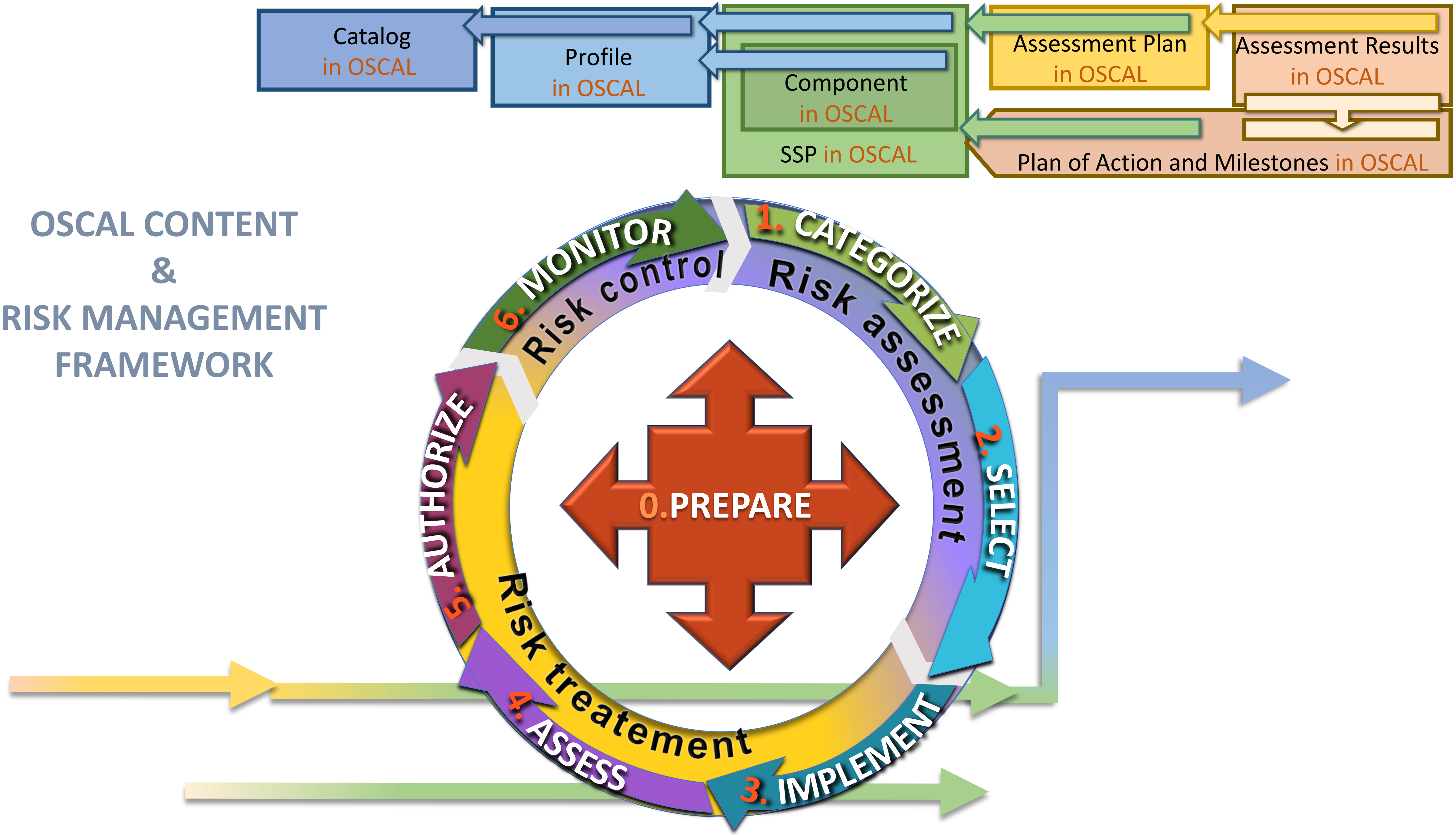
OSCAL Models vs OSCAL Content



OSCAL Content vs OSCAL Tools



OSCAL CONTENT & RISK MANAGEMENT FRAMEWORK



Catalog in OSCAL

Profile in OSCAL

Component in OSCAL

SSP in OSCAL

Assessment Plan in OSCAL

Assessment Results in OSCAL

Plan of Action and Milestones in OSCAL

0.PREPARE

1. CATEGORIZE

2. SELECT

3. IMPLEMENT

4. ASSESS

5. AUTHORIZE

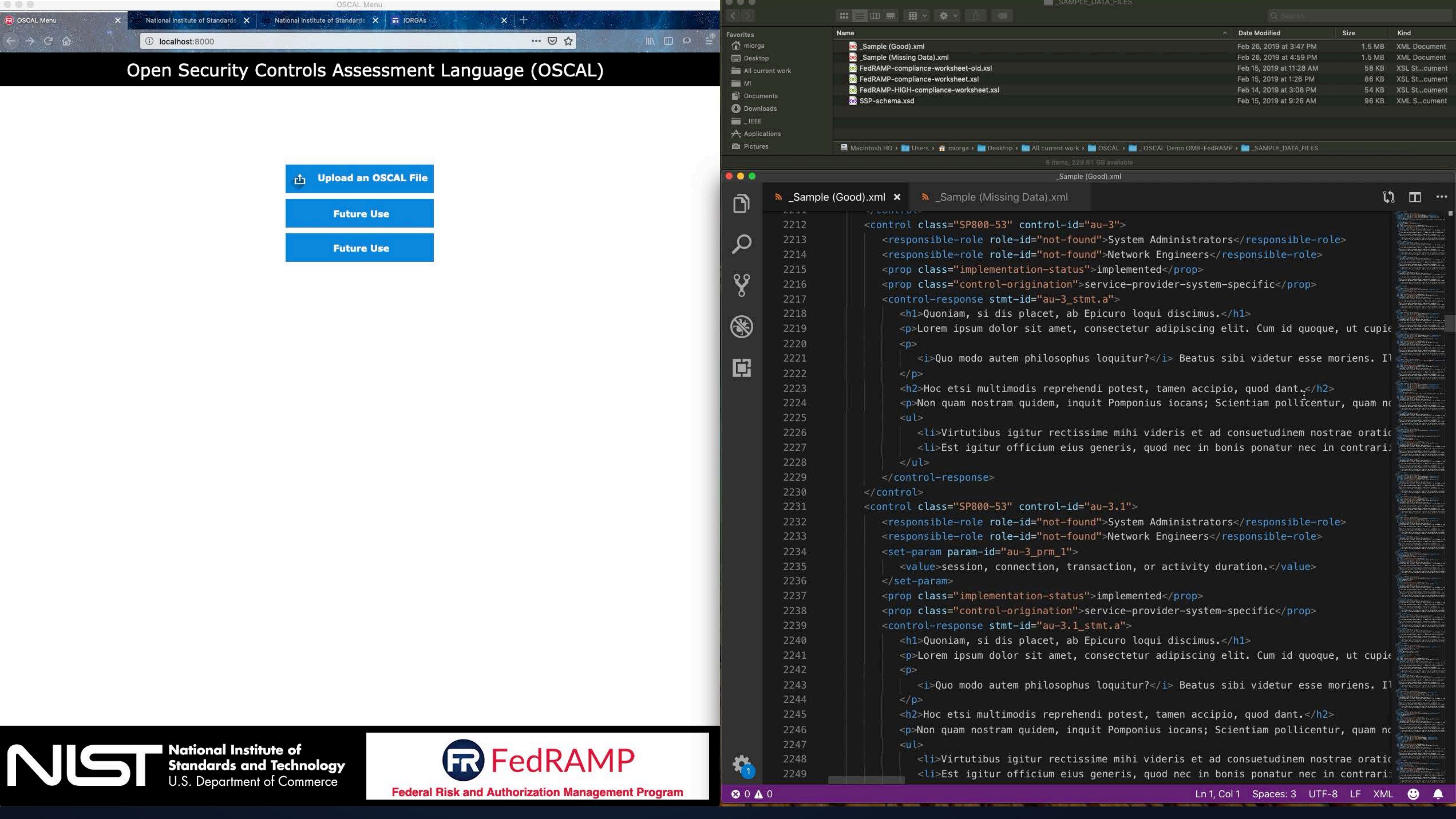
6. MONITOR

Risk assessment

Risk treatement

Risk control

Show an


OSCAL Menu
National Institute of Standards
National Institute of Standards
IORGAs
localhost:8000

Open Security Controls Assessment Language (OSCAL)

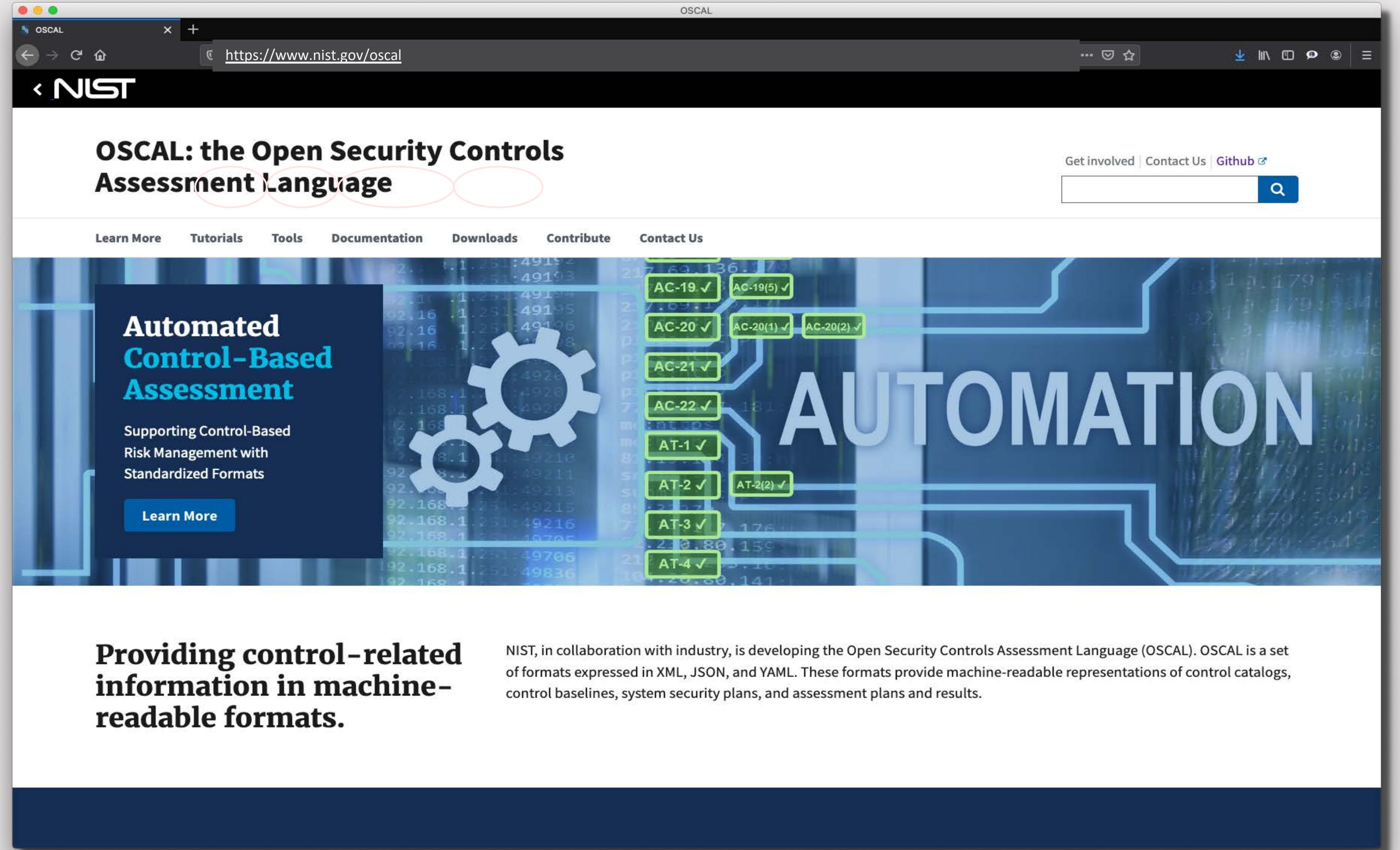
Upload an OSCAL File
Future Use
Future Use
National Institute of Standards and Technology
U.S. Department of Commerce
FedRAMP
Federal Risk and Authorization Management Program
_SAMPLE_DATA_FILES
Favorites
miorga
Desktop
All current work
MI
Documents
Downloads
_IEEE
Applications
Pictures

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

```
</control>
<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
```



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.

Summary of OSCAL Benefits

- **Automated assessment planning and pre-validation:**
  - Perform many SSP validation checks automatically
  - Generate lists of who to interview about which topics
  - Configure scanning tools from inventory
- **Perform faster, higher quality assessments:**
  - Automatically convert tool findings to assessment report syntax and/or POA&M entries
  - Automatically populate report views
  - Streamline entire review process
- **Ability to self test prior to submission:**
  - Automatically identify many issues prior to submission

- ❑ **Create and maintain artifacts more efficiently**
  - ❑ SSP, system inventory, POA&M
- ❑ **Perform many validation checks before package submission**
  - ❑ Self-service feedback on compliance issues and common mistakes
- ❑ **Create and release validation checks**
- ❑ **Receive higher-quality packages due to self-service feedback**
- ❑ **Shift level of effort away from compliance and toward risk management**
  - ❑ Eliminate "busy work" aspect of reviews
  - ❑ Focus on human attention where human judgement is most needed
- ❑ **Automated workflows and tracking**
- ❑ **Tool interoperability**
- ❑ **Data Analytics**

Publicly Available Resources

Documentation:

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

Example:

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

FedRAMP catalog and baselines (XML & JSON):
https://github.com/usnistgov/OSCAL/tree/master/content/fedramp.gov

FedRAMP Automation:

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

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

Tools

OSCAL Kit: https://github.com/docker/oscalkit

OSCAL GUI: https://github.com/brianrufgsa/OSCAL-GUI

OSCAL Adopters

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

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

Questions?