



Open Security Controls Assessment Language (OSCAL)

Lunch with the OSCAL Developers

David Waltermire

National Institute of Standards and Technology

Teleconference Overview

- Ground Rules
- OSCAL Status Summary (5 minutes)
- Question and Answer / Discussion
 - Submitted questions will be discussed
 - The floor will be open for new questions and live discussion

OSCAL Lunch with the Developers

Purpose:

- Facilitate an open, ongoing dialog with the OSCAL developer and user communities to promote increased use of the OSCAL models

Goals:

- Provide up-to-date status of the OSCAL project development activities
- Answer questions about implementing and using the OSCAL models, and around development of OSCAL model-based content
- Review development priorities and adjust priorities based on community input
- Help the OSCAL community identify development needs

Ground Rules

- Keep the discussion respectful
 - Using welcoming and inclusive language
 - Being respectful of differing viewpoints and experiences
 - Gracefully accepting constructive criticism
 - Focusing on what is best for the community
 - Wait for one speaker to finish before speaking - one speaker at a time
- Speak from your own experience instead of generalizing ("I" instead of "they," "we," and "you").
- Do not be afraid to respectfully challenge one another by asking questions -- focus on ideas.
- The goal is not to always to agree -- it is to gain a deeper understanding.

OSCAL Version 1 Milestones

Milestone	Focus	Sprints	Status	Date
Milestone 1	Catalog and Profile Models	1 to 21	Completed	6/15/2019
Milestone 2	System Security Plan (SSP) Model	6 to 23	Completed	10/1/2019
Milestone 3	Component Definition Model	6 to ~30	Completed	May 2020
Release Candidates	Provide a web-based specification / Model Improvements	24 to ~35	In Progress	~November 2020
Full Release	Based on Community Feedback	34 to 36	Planned	By end of 2020
Ongoing Maintenance	Minor and bugfix releases as needed	Additional Sprints	Planned	Ongoing

Current Sprint: 36 (<https://github.com/usnistgov/OSCAL/projects/35>)

All Current NIST OSCAL Work: <https://github.com/orgs/usnistgov/projects/9>

Progress towards the Release Candidate

<https://github.com/usnistgov/OSCAL/tree/metaschema-m4-integration>

Work Completed

- Improved all model overviews
- All models have been upgraded to Metaschema M4 revision
- Schema Production
- Content Converter Production
- Significant model changes

Work Remaining

- Correlation constraints (need review)
- Generalize allowed values from FedRAMP
- Generation of Model and model outline documentation
 - Hugo integration
 - XML docs
 - JSON docs
- Addressing remaining model issues
- M3 -> RC1 content updater
- Update existing content in [oscal-content](#) GitHub repo

OSCAL 1.0.0 RC1 Milestone: <https://github.com/usnistgov/OSCAL/milestone/8>

Reasons for delay of OSCAL 1.0.0 RC1

- Received a good amount of community feedback on the OSCAL models
 - We have a very engaged community. This is a good thing.
 - Currently working through this feedback
- Work on the final SP 800-53 rev 5 and SP 800-53B content
- Focus on improving generated XML and JSON documentation
- Work on making all OSCAL models consistent

All of this will result in a better OSCAL 1.0.0!

Review of Current/Completed Work

On Github: <https://github.com/usnistgov/OSCAL>

Help Needed

- Please review pull requests and comment on issues you are interested in.
- Need more model review: schemas, documentation gaps, etc.

Open Floor

What would you like to discuss?

What questions do you have?

Should we be covering anything differently?

Thank you

Next Lunch with Devs:

December 3rd, 2020

12:00 Noon EST (4:00 PM UTC)

OSCAL Repository:

<https://github.com/usnistgov/OSCAL>

Project Website:

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

How to Contribute:

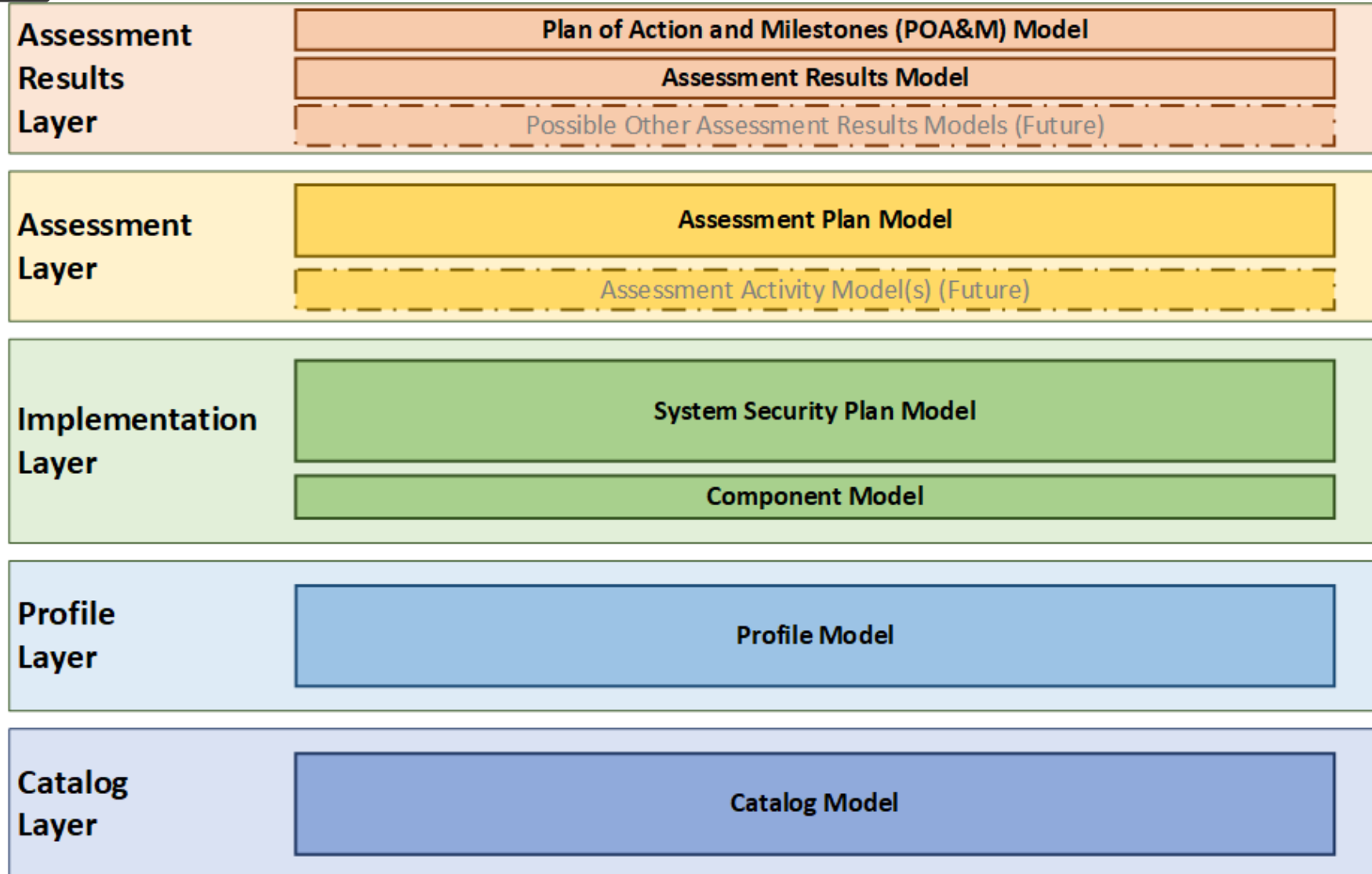
<https://pages.nist.gov/OSCAL/contribute/>

Contact Us: oscal@nist.gov

On Gitter:

<https://gitter.im/usnistgov-OSCAL/Lobby>

Three New OSCAL Models



POA&M

- Based on FedRAMP POA&M

Assessment Results

- Based on FedRAMP Security Assessment Report (SAR)

Assessment Plan

- Based on FedRAMP Security Assessment Plan (SAP)