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)
- Issues Needing Help from the Community
- 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 **~33**	**In Progress**	~**August 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: 31 (https://github.com/usnistgov/OSCAL/projects/30)

OSCAL v1 Milestone 3 Release

- A new component definition model, provide a description of the controls supported by a specific implementation of a hardware, software, or service; or by a given policy, process, procedure, or compliance artifact (e.g., FIPS 140-2 validation).
- Creation of draft models for the assessment and assessment result layers. Drafts of the assessment plan, assessment results, and plan of action and milestones (POA&M) models were created. These drafts were slated for the OSCAL v2 release cycle and are being released early as drafts ahead of schedule.
- Updated stable versions of the OSCAL catalog, profile, and system security plan (SSP) models.
- New OSCAL content in XML, JSON, and YAML formats for the draft NIST SP 800-53 revision 5 catalog.
- Updated content in OSCAL XML, JSON, and YAML formats for the NIST SP 800-53 revision 4 catalog, and for the three NIST and four FedRAMP baselines.
- Provides tools to convert OSCAL catalog, profile, and SSP content between OSCAL XML and JSON formats, and to up convert content from milestone 2 to milestone 3.

The NIST OSCAL team is very thankful for all of the great feedback we have received!

Review of Current/Completed Work

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

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:

July 2nd, 2020

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

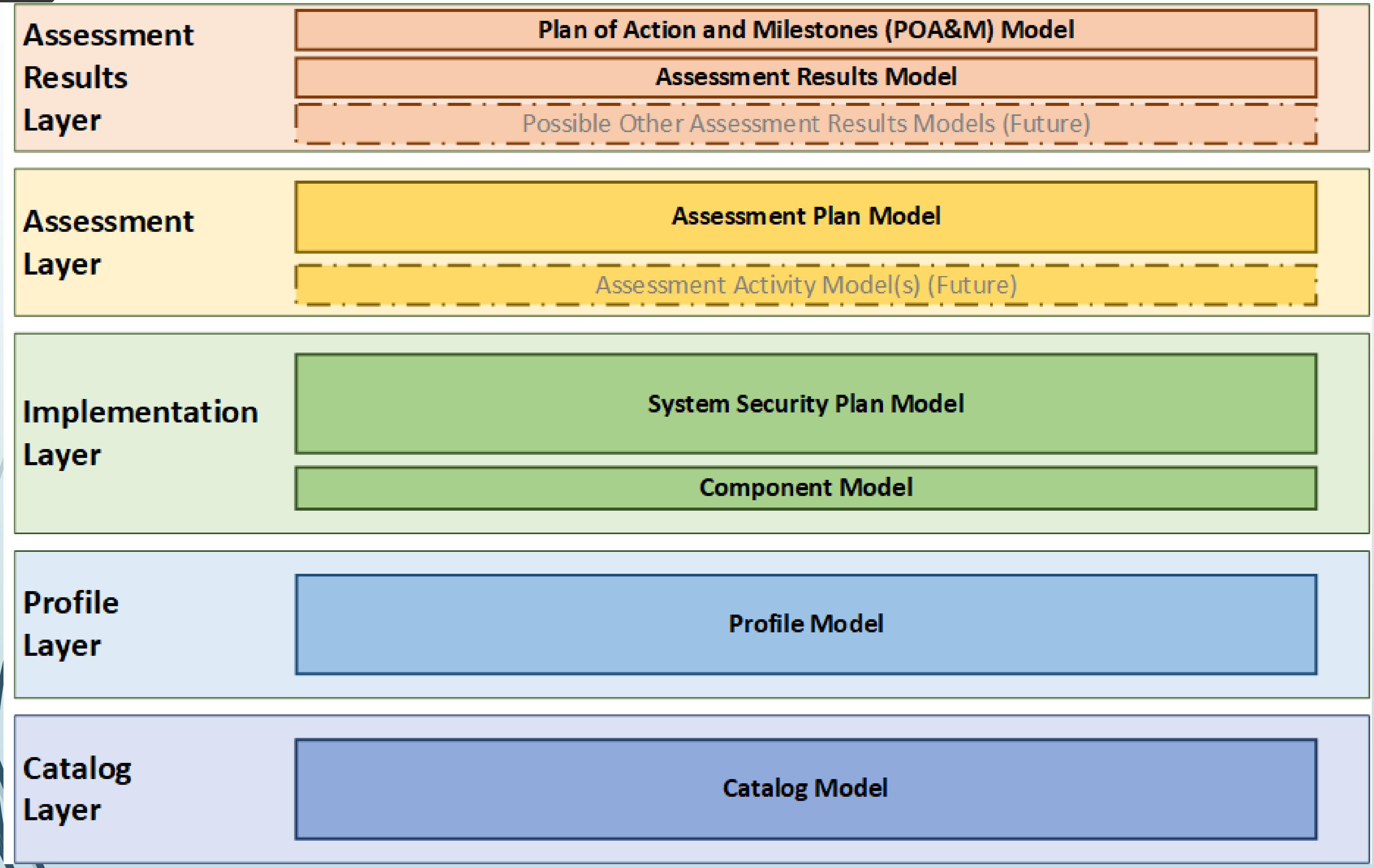
OSCAL Repository:
https://github.com/usnistgov/OSCAL

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

How to Contribute:
https://pages.nist.gov/OSCAL/contribute/

Contact Us: oscal@nist.gov

Three New OSCAL Models



Assessment Results Layer

- Plan of Action and Milestones (POA&M) Model
- Assessment Results Model
- Possible Other Assessment Results Models (Future)

Assessment Layer

- Assessment Plan Model
- Assessment Activity Model(s) (Future)

Implementation Layer

- System Security Plan Model
- Component Model

Profile Layer

- Profile Model

Catalog Layer

- Catalog Model

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)