Open Security Controls Assessment Language (OSCAL)

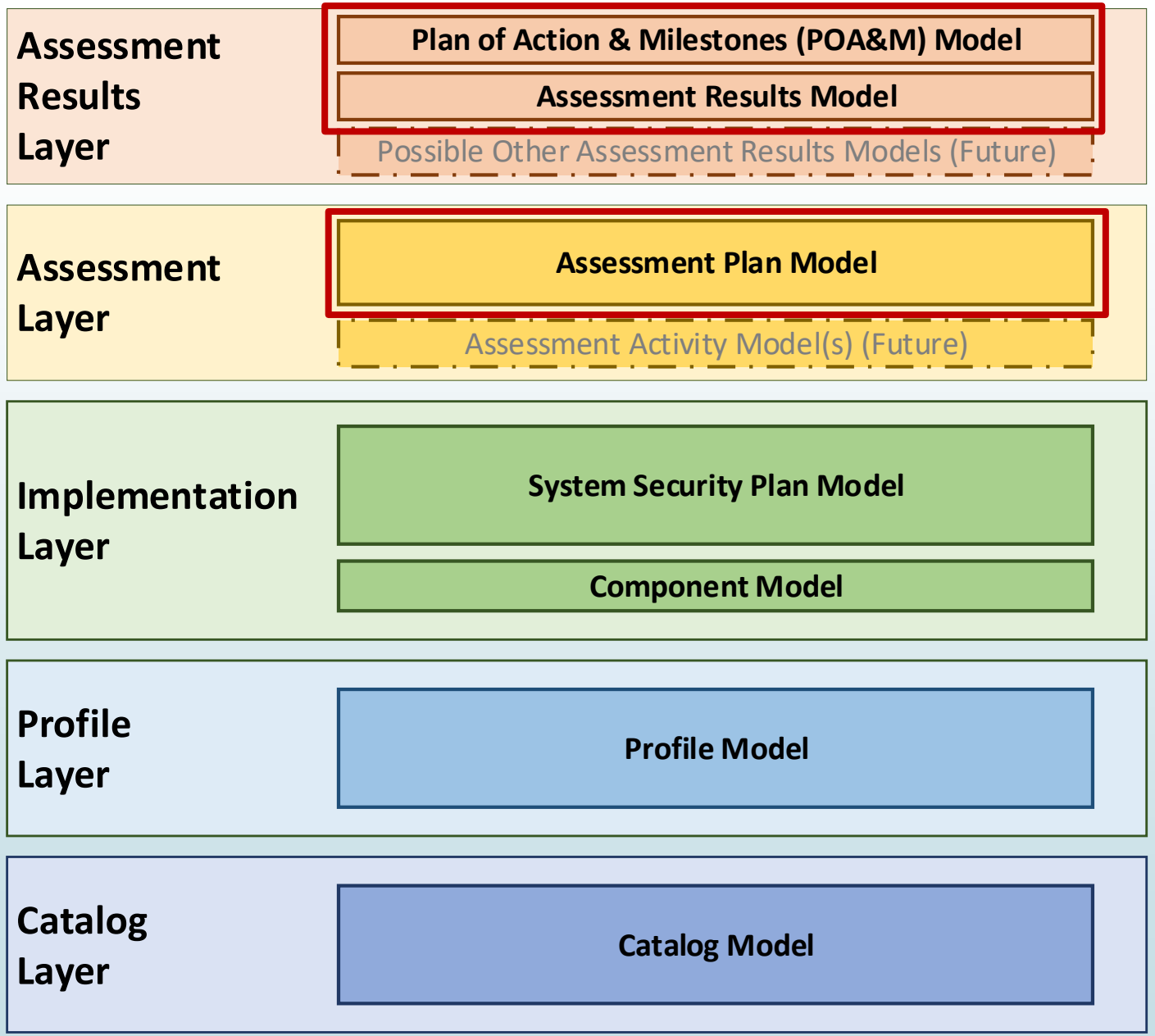
Assessment Plan
Assessment Results
Plan of Action and Milestones

Brian J. Ruf, CISSP, CCSP, PMP
National Institute of Standards and Technology

Overview

Three New Models:

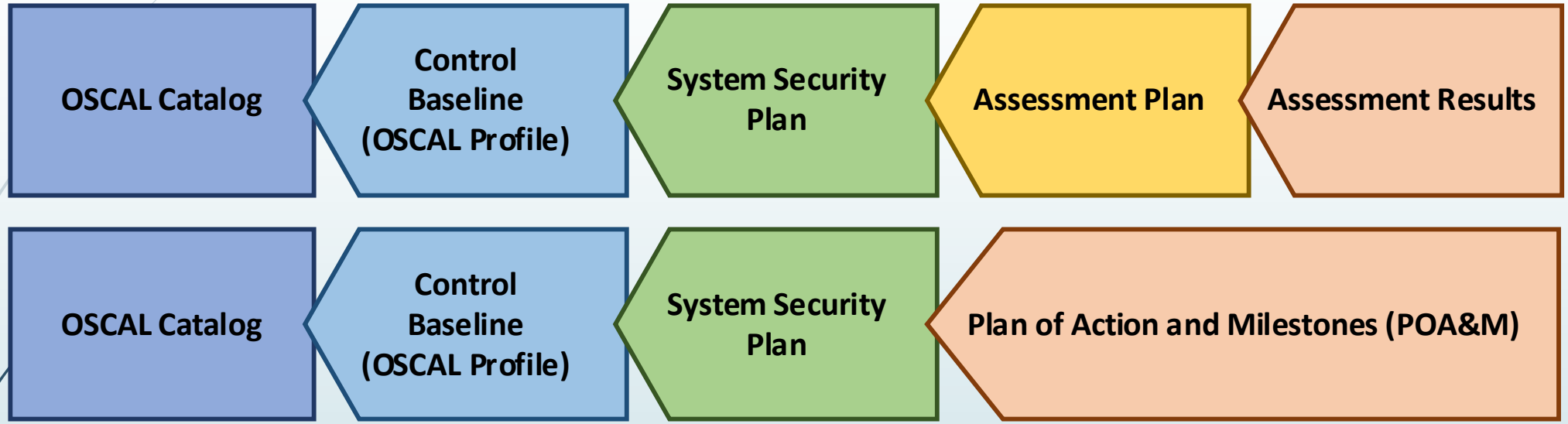
- Assessment Plan
- Assessment Results
- Plan of Action and Milestones



Background

- Assessment Layers were intended to be addressed in OSCAL 2.0
- FedRAMP has an immediate need to receive a complete ATO package in OSCAL
- NIST and FedRAMP agreed to expand OSCAL now to enable OSCAL modeling of FedRAMP SAP, SAR, and POA&Ms
- Developed these with FedRAMP as the focus, but also in anticipation of other uses, such as continuous assessment
- Additional assessment layer features will still be addressed in OSCAL 2.0, such as additional mechanism to automate assessment inspections and testing.

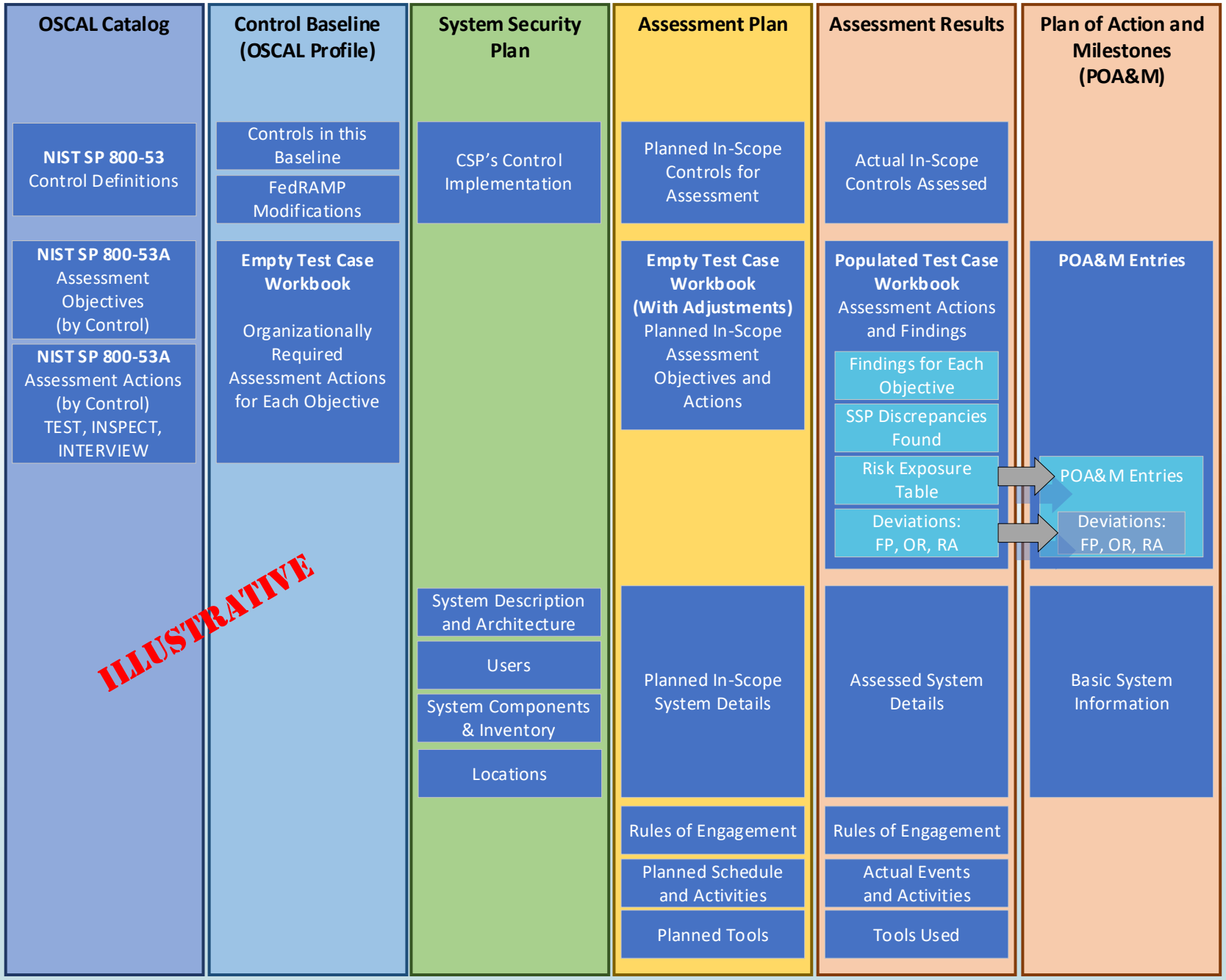
Importance of Import



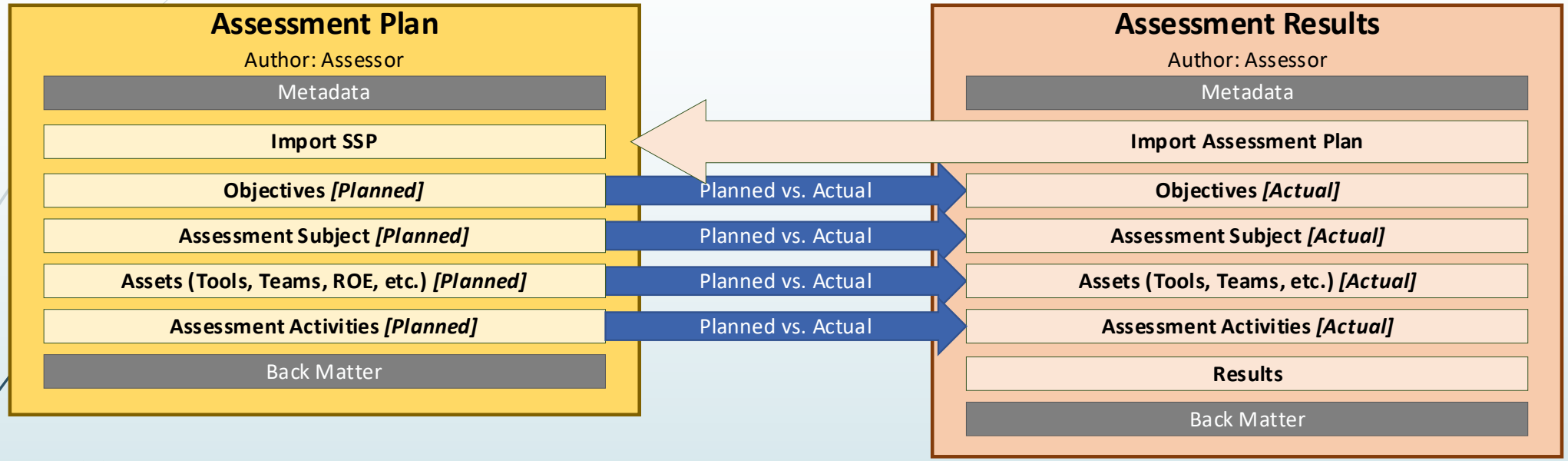
- OSCAL is designed for traceability
- In most cases:
  - Models to the right refer to content in models on the left, instead of duplicating content
  - There are a few exceptions

Importance of Import

- FedRAMP Example
  - The SSP refers to the profile and catalog for control definitions
  - The Assessment Plan and Results refer to the SSP for system description and architecture



Overlapping Syntax (AP and AR)



Traditional Snapshot Approach

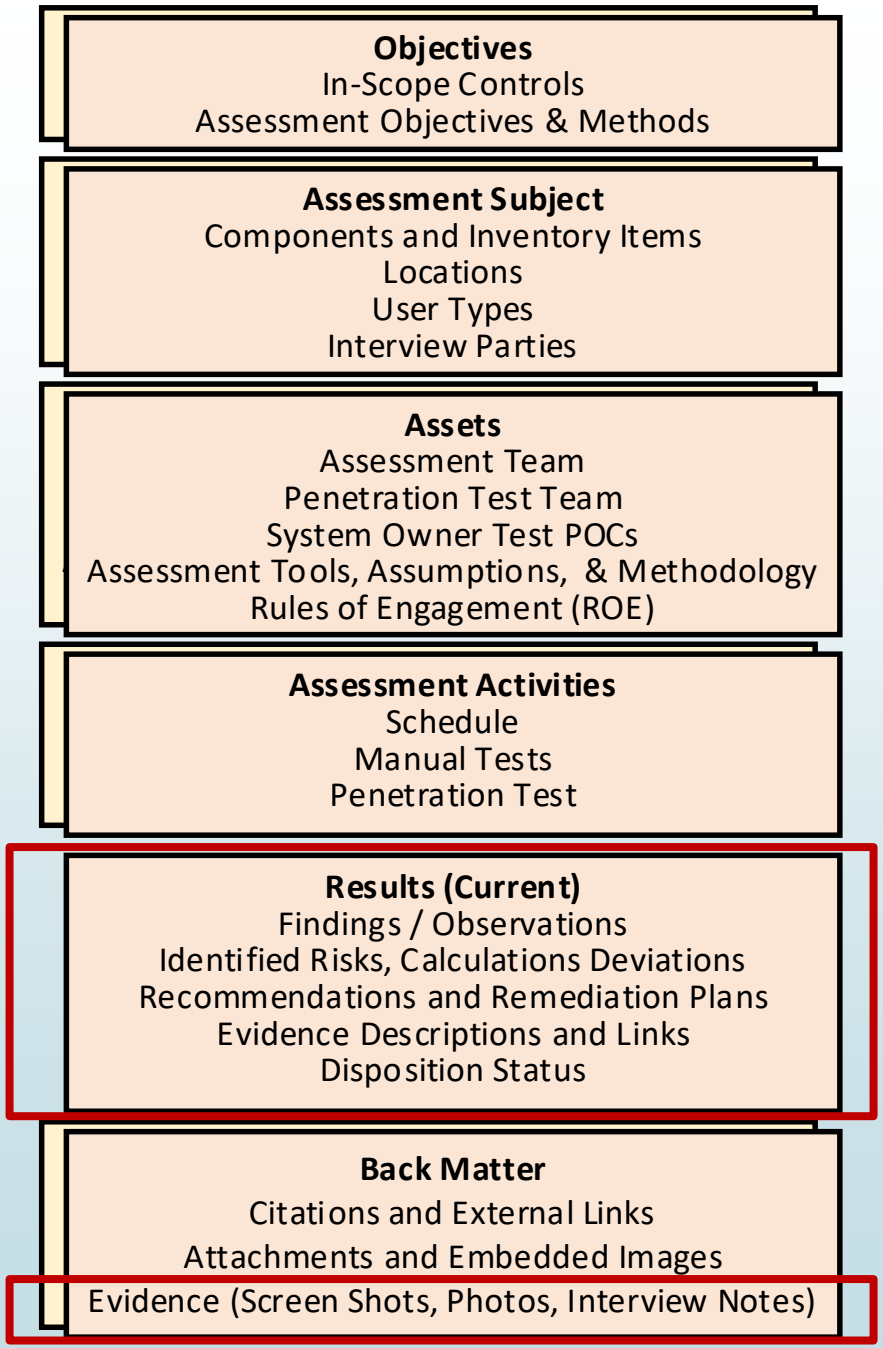
- **Assessment Plan**: What the assessor plans to do
- **Assessment Results**: What the assessor actually did

Continuous Assessment Approach

- **Assessment Plan**: What should be tested/inspected, how, and in what frequency
- **Assessment Results**: Time-slice of results

Assessment Plan and Assessment Results

- **Common to AP and AR:**
  - **Objectives**
  - **Assessment Subject**
  - **Assets**
  - **Assessment Activities**
  - **Back Matter (general)**
- **Unique to AR:**
  - **Results**
  - **Evidence in Back matter**



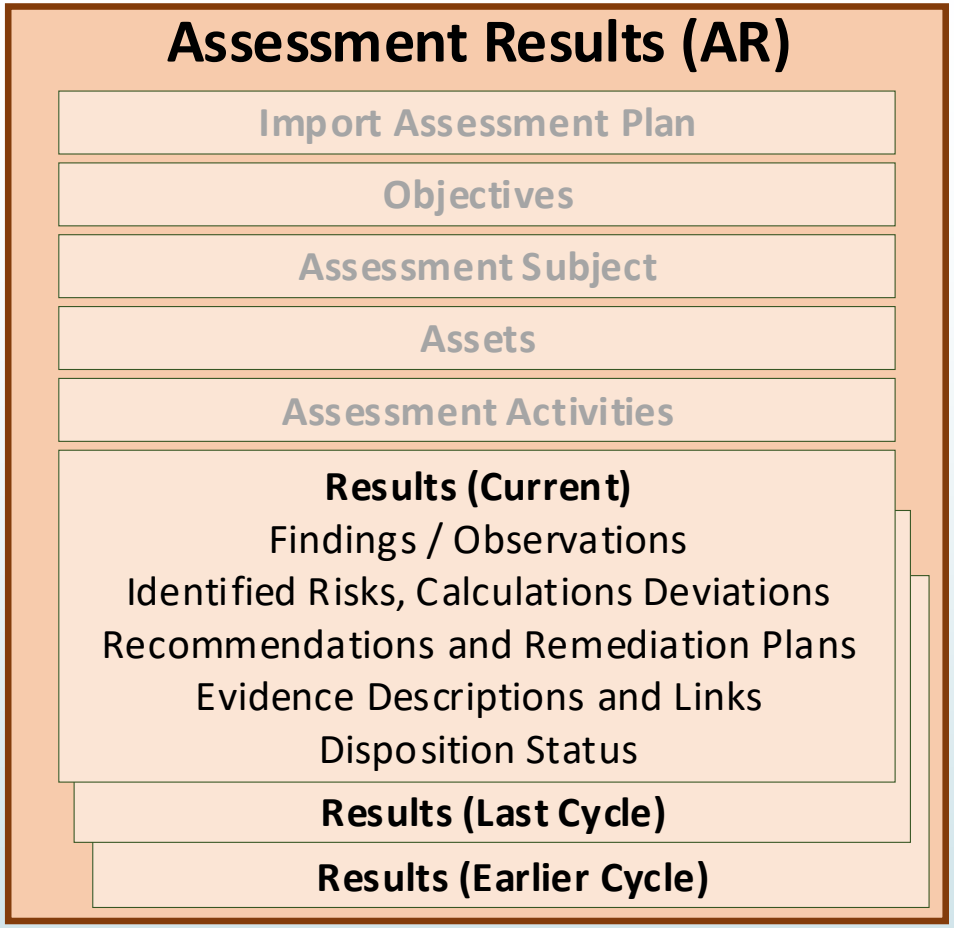
Assessment Results: Time Slices

Traditional Snapshot Approach

- Entire current assessment in one Results assembly
- Each past assessment cycle in its own results assembly

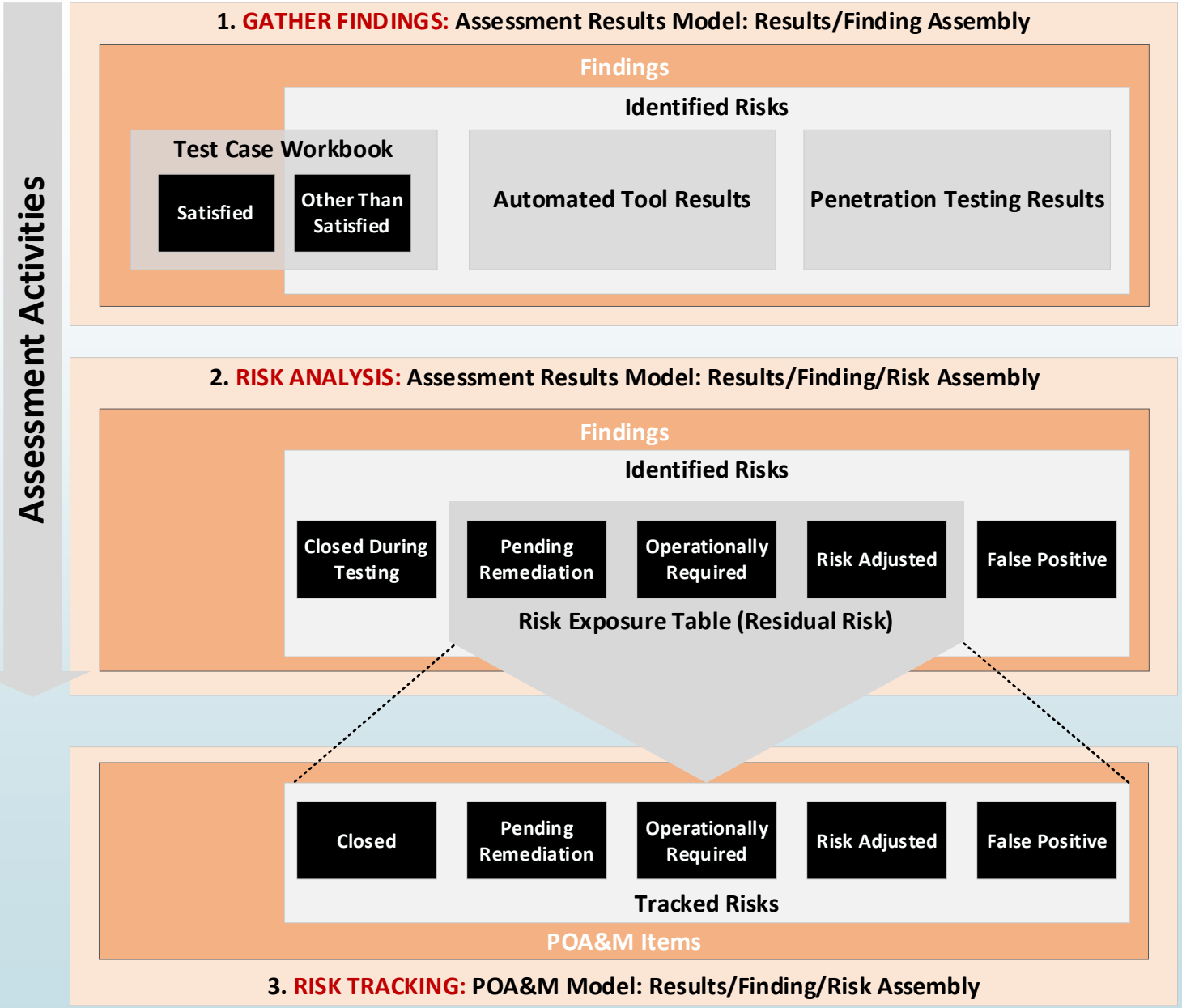
Continuous Assessment Approach

- Each Results assembly is a snapshot in time
- Example: If testing once per hour, each results assembly represents the testing for that hour

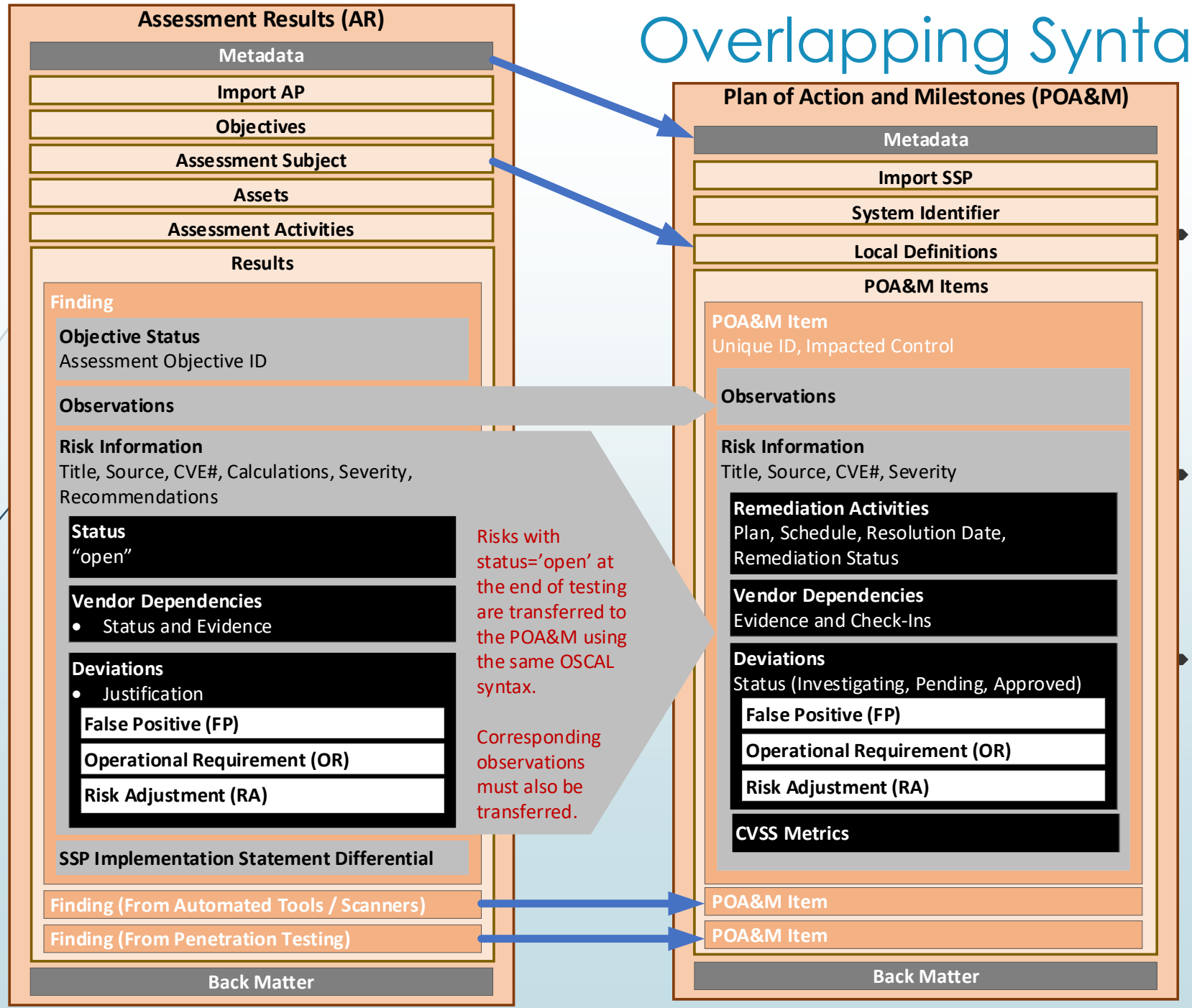


Findings, Risks, Analysis, and Flow

1. Gather findings. Some findings demonstrate compliance. Other findings demonstrate a lack of compliance and represent a risk.
2. While performing risk analysis, some risks are closed during the assessment period. Others are identified as a false positive. Some open risks have mitigating factors, resulting in a risk adjustment. The remaining open and adjusted risks are typically populated in a risk exposure table.
3. All residual risks are typically entered into the POA&M by the system owner, where they are tracked until closure.



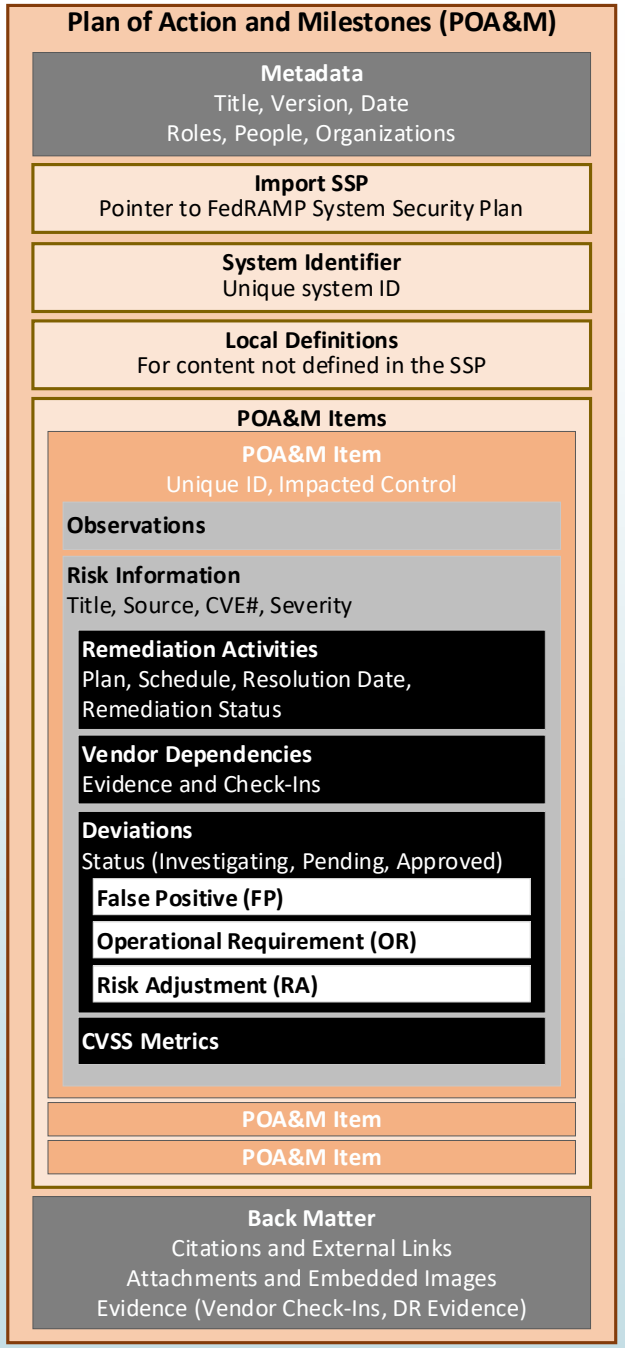
Overlapping Syntax (AR and POA&M)



- Typically all remaining assessment risks are entered into the POA&M. (not closed during testing, and not a verified FP)
- To facilitate this, the syntax the same for an individual AR finding and an individual POA&M item.
- While some detail, such as objective status, may be filtered, it can also travel to the POA&M along with the risk information if appropriate.

POA&M Model

- Ideally the POA&M imports an SSP.
- The System Identifier is used when a POA&M is delivered without its corresponding SSP
  - Example: Monthly Continuous Monitoring (ConMon) delivery of a POA&M where an SSP is only delivered annually.
  - This enables another tool to re-link the POA&M and a previously delivered SSP.
- Scanning tools and missing SSP content are defined in the Local Definitions assembly.
- The structure provides robust remediation planning and tracking activities.
- The structure also provides risk metrics and deviation management for multiple different compliance frameworks. OSCAL enables these to co-exist in a single POA&M item entry.



Questions?
Thank you!

We want your feedback!

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

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

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

FedRAMP Implementation Guides
https://github.com/gsa/fedramp-automation **(Available in July)**

Thank you

We want your feedback!

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

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

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