AWS and Telos Lessons Learned from Submitting the First OSCAL SSP

Matthew Donkin

Information Assurance Manager
U.S. Government Security & Compliance

Stephanie Lacy

Senior Solutions Architect
Telos

AWS OSCAL Implementation Lessons Learned

OSCAL Format Challenges

- **Aligning all information correctly from various documentation types**
  - SSPs are written differently and have appendices
  - Plan of action and milestones (POA&M) are written with various levels of information
  - Ensuring all pertinent data is in the correct layout for the OSCAL export

AWS OSCAL SSP Challenges

- **AWS System Security Plan has multiple parts for each boundary**
  - Commercial offerings has one main and three appendices
  - GovCloud has one main and three appendices
  - Multiple OSCAL export files depending on IaaS, PaaS, or SaaS offerings and boundary requirements
- **Solution: Adding OSCAL appendices as separate files**
  - Temporary solution as we work to find a better way to interpret the SSP into a FedRAMP acceptable single OSCAL format file

OSCAL Implementation Challenges

- **Multiple workstreams input**
  - For maximum benefit of the OSCAL format input from 4 different organizations within AWS
  - Creates issues with managing workflow
- **Erroneous information requirements that are not applicable to hyper-scaling CSPs**
  - How many users at any one time on the cloud
  - Roles of each individual working within the environment

OSCAL Successes

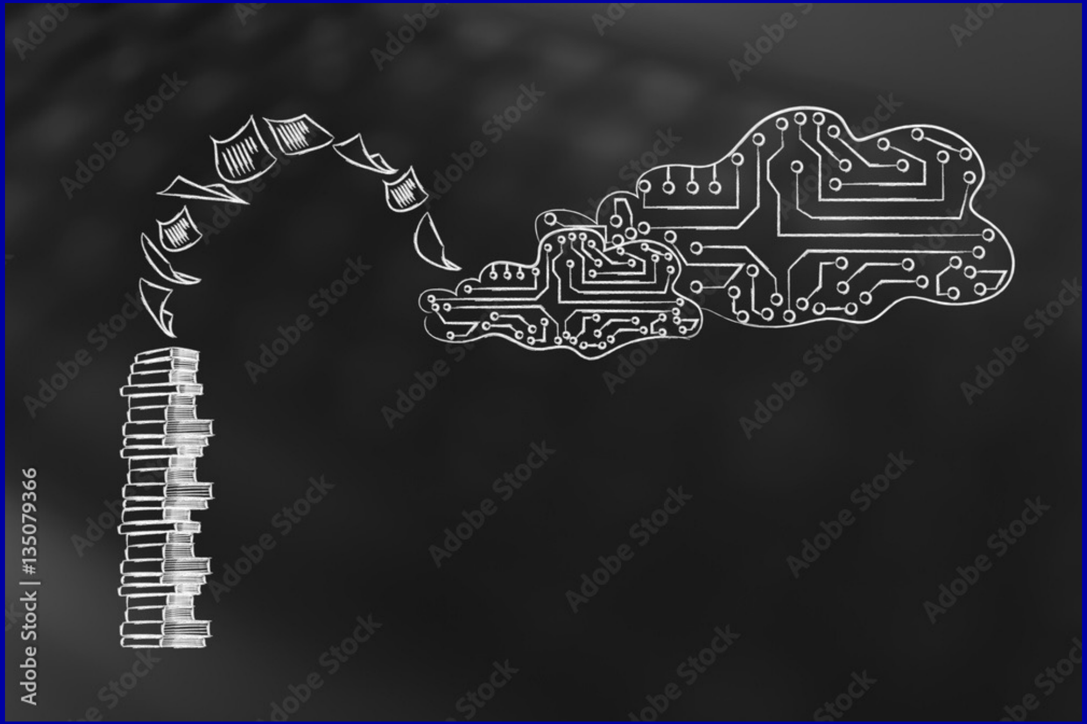
- AWS, in collaboration with Telos, was the first CSP to provide an OSCAL SSP to FedRAMP

- Able to provide feedback to industry partners to suggest improvements to FedRAMP OSCAL template

- Partner with Accenture (3PAO) to pilot a complete OSCAL authorization package by Q4 2022
  - System Assessment Plan
  - System Assessment Report

OSCAL Authorization Package Timeline

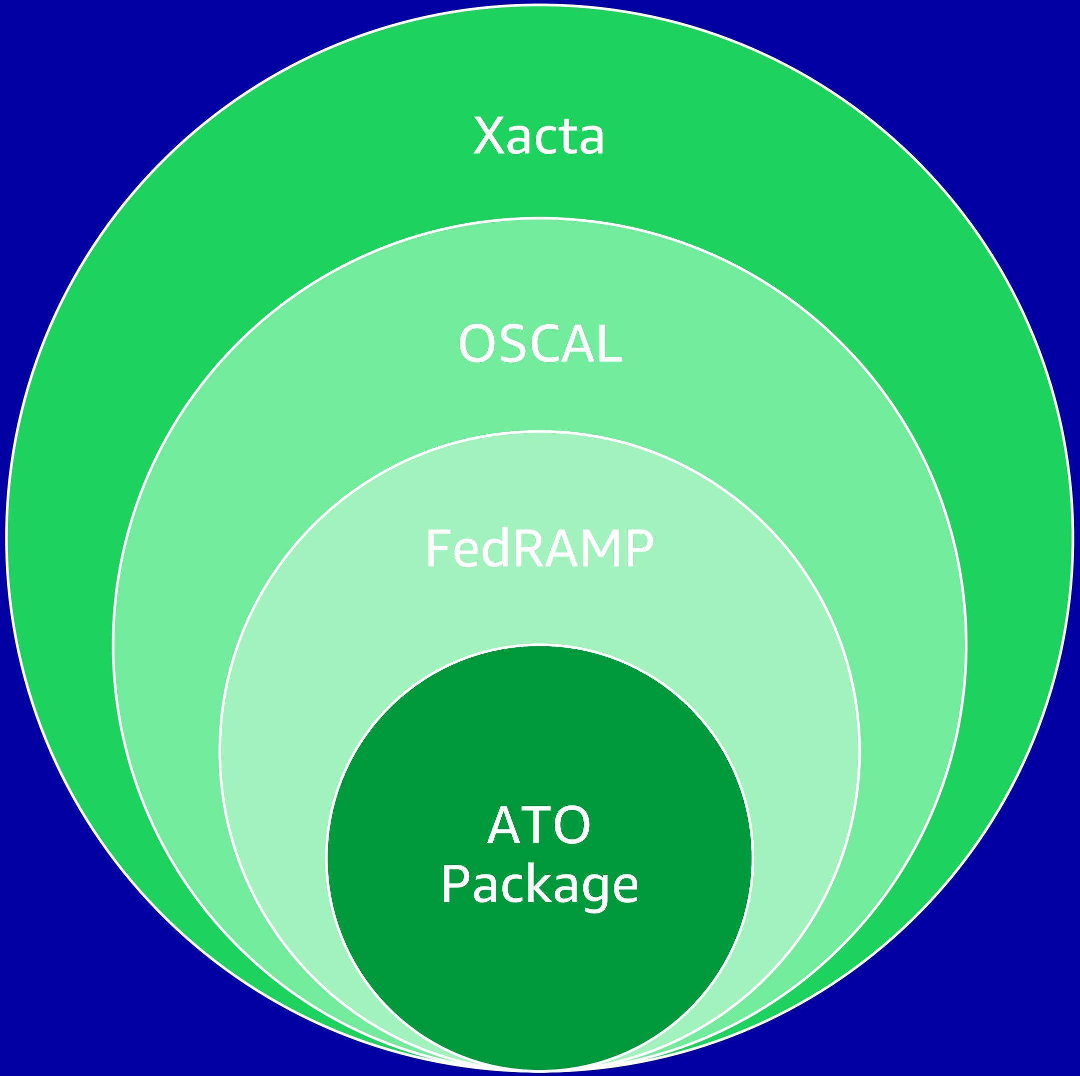
- **System Security Plan (SSP)**
  - Status: Complete
- **Security Assessment Plan (SAP)**
  - Status: In progress
  - EDC: Q4 2022
- **Security Assessment Report (SAR)**
  - Status: In progress
  - ECD: Q4 2022
- **Plan of Action and Milestones (POA&M)**
  - Status: In progress
  - ECD: Q4 2022



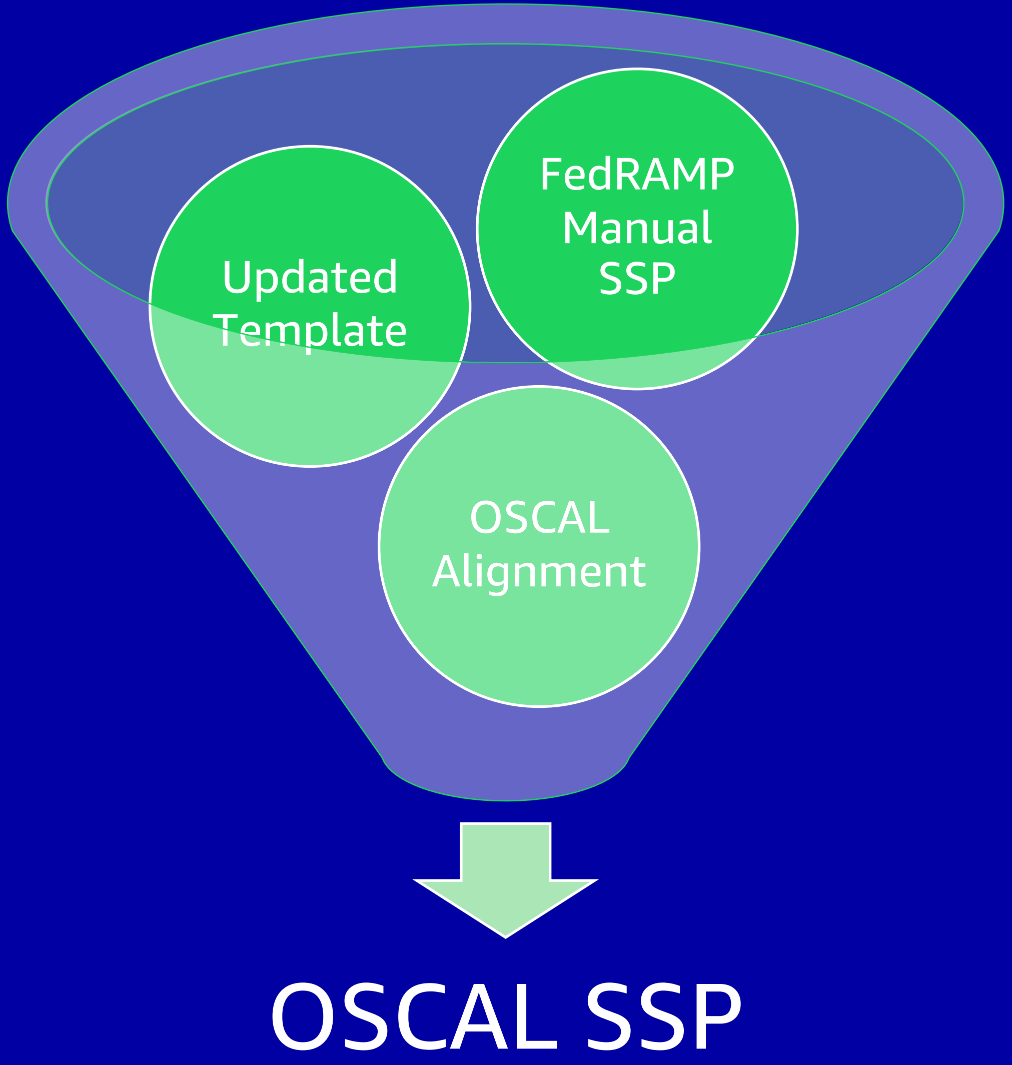
Telos Xacta® OSCAL Implementation Lessons Learned

Challenges

- Xacta's Data Exchange Model (XDE) Developed before OSCAL Solution
- Unifying strategies between use cases to balance future deployments.
- Converting from Manual Process to OSCAL
- Protecting future use-cases
- Supporting the implementation of a mature product as it moves through development



Successes



Leverage bots, api ingests, form posts, and other technologies to ingest data from various customer sources into Xacta

Modernize FedRAMP template

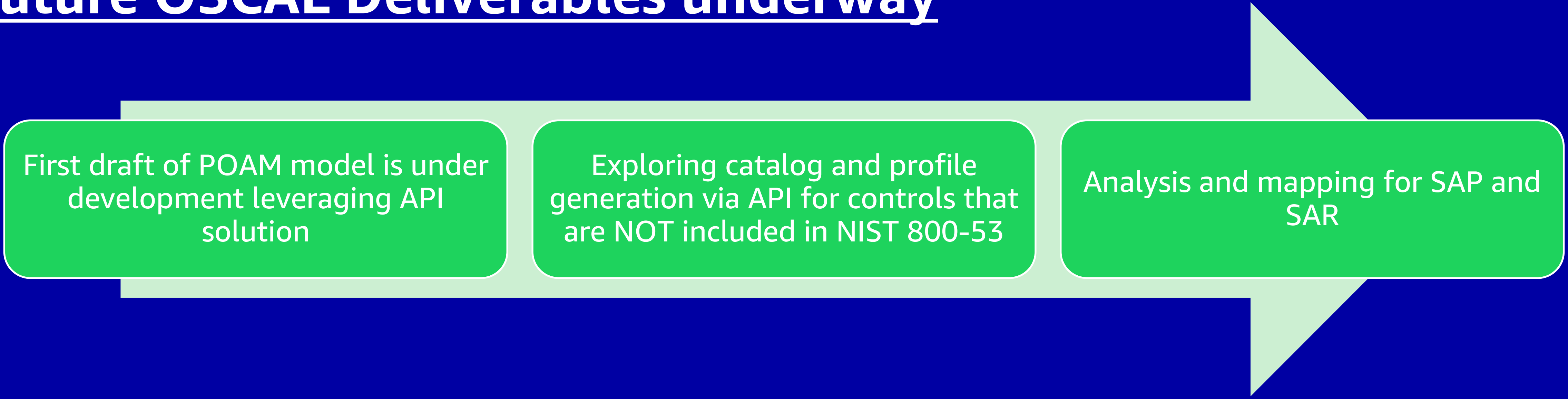
Validating outputs leveraging NIST Schema, and FedRAMP Validator

Releasing new API endpoints to capture OSCAL without hardcoding

Moving Forward

- Feedback loop process with NIST and FedRAMP to address unique challenges
- Catalog for NIST 800-53 controls is provided by NIST

Future OSCAL Deliverables underway



First draft of POAM model is under development leveraging API solution

Exploring catalog and profile generation via API for controls that are NOT included in NIST 800-53

Analysis and mapping for SAP and SAR

Questions?

Thank you!

Matthew Donkin

Information Assurance Manager
U.S. Government Security & Compliance
LinkedIn:

Stephanie Lacy

Senior Solutions Architect
Telos