Amazon Web Services and OSCAL

A Brief Overview

Matthew Donkin, James Mueller, Douglas Boldt
3/2/2022
# Table of contents

- AWS Implementation
- Customer Benefits
- AWS Documentation
- Improving Customer Experience
- Challenges Implementing OSCAL
- Closing Thoughts
- Questions?
AWS Implementation of OSCAL
AWS Implementation

- **Xacta (Telos) Governance, Risk Management and Compliance (GRC) Tool**
  - Provide *multiple classification* levels of OSCAL formatted authorization packages

- **OSCAL Template**
  - FedRAMP: [https://github.com/GSA/fedramp-automation](https://github.com/GSA/fedramp-automation)

- **Automate portions of authorization packages**
  - Reduce *human error* in documentation
  - Decrease timelines for authorization package preparation
  - Compress third party assessor organizations (3PAOs) review timeline
Customer Benefits
Customer Benefits

• **Reduce timeline for AWS service authorizations**
  • FedRAMP
  • DoD CC SRG Impact Levels 4 and 5

• **Simplify security control document handling and ingestion**
  • Eliminate manual copy and paste of information
  • Reduce review time for new security control documentation updates

• **Streamline system Authorization to Operate (ATO) process**
  • Introduction of *machine-readable* representations of control catalogs, control baselines, system security plans, and assessment plans and results.
  • Improve transparency into the ongoing security posture of the security control providers
AWS Documentation
Documentation

- **System Security Plan (SSP)**
  - 2 SSPs
  - 12 Monthly updates
  - 1 annual assessment
  - GovCloud SSP is 735 pages

- **Customer Responsibility Matrix (CRM) and Customer Configuration Guides (CCG)**
  - 24 Monthly updates per year
  - 27,123 projected 2022 downloads

- **Total customer document downloads for 2021:** 34,763
Improving Customer Experience
Customer Experience

• **Current process**
  • Request access to digital rights management solution
  • Manually copy requisite security documentation into GRC
  • Manually update documentation on a monthly basis
  • Estimated 4,160 workforce hours per year to create and maintain ATO package

• **OSCAL simplification**
  • Request access to GRC (Xacta)
  • Download OSCAL authorization package
  • Upload into OSCAL enabled GRC solution
  • Estimated 20-40 workforce hours per year to create and maintain ATO package
Challenges Implementing OSCAL
Challenges

• **Adoption**
  • For OSCAL to work it has to have adoption across government and industry

• **Integration**
  • Challenges with various existing tools to integrate OSCAL format

• **Collaboration**
  • Different templates between CSPs and GRCs
  • Differing priorities between government and industry
Closing Thoughts

• OSCAL potential
  • Enable faster more accurate authorization packages
  • Decrease customer’s security documentation burden
  • Improve transparency into CSP ongoing security posture
  • Reduce service authorization timelines by 2-4 weeks
  • Decrease estimated customer documentation burden by magnitudes
  • Provide an overall better customer experience with security documentation

• OSCAL Challenges
  • OSCAL must have widespread adoption to be successful
  • Integration into existing tools can be difficult
  • Unique templates may cause issues with data transfer between systems
Questions?