Virtual Room #3

Hosted By: Jet Ryan, Solutions Architect, Telos Corporation

Disclaimer: Portions of the event may be recorded and audience Q&A or comments may be captured. The recorded event may be edited and rebroadcasted or otherwise made publicly available by NIST. By attending this event, you acknowledge and consent to having your conversation recorded.

oscal2022@nist.gov
conferences@nist.gov
Getting a Head Start on Automating your FedRAMP ATO using OSCAL in Xacta360

March 2, 2022
INTRODUCTION

Jet Ryan
Solutions Architect - OSCAL Lead
Telos Corporation
Xacta® 360

- Xacta has existed as a compliance management platform since 2000
- Pre-built workflows for frameworks like FedRAMP and NIST RMF
- Customization without code, optimized for cloud security assessments
- Reduces time and dependencies in the assessment and authorization process
What’s Next?

How can we push the limits of compliance automation?
Open Security Control Assessment Language (OSCAL) is a data centric framework with the goal of standardizing the process for documenting and accessing security controls.

- OSCAL enables movement at machine speed, allowing for faster authorization.
- Advantages to roles across the authorization process.
- Xacta360 will “hold the door open” to get users started in compliance as code.
- Creation of “OSCAL enabled” workflows with pre-built mappings.
- One click OSCAL export to generate an OSCAL package.

Our Vision: Accelerated ATO Enabled by OSCAL.
OSCAL From the Bottom Up

- Xacta360 leverages OSCAL FedRAMP Controls Catalogs
- Xacta360 references OSCAL FedRAMP Baseline Profiles
- Started from SSP layer
- Plans are in motion to complete the SSP layer and interlink with other models
Current Release

- Mapped the OSCAL model for FedRAMP on the Xacta360 FedRAMP project
- Included the Metadata, System Characteristics, and System Implementation
  - Roles
  - System users
  - Ports, protocols, and services
  - Equipment inventory
  - System environment
  - Location
  - + more
In Development

• Inclusion of Controls implementation section
  • Responsible roles
  • Control parameters
  • Implementation status
  • Controls Origination
  • + more
• Resolve variation in control models
• Finalize what is accepted in terms of an OSCAL package
Near future:
• Support controls catalog layer and profile layer on SSP export for dynamic OSCAL
• Completion of the SSP Layer with inclusion of Back-matter, import of profile, and leveraged authorizations

Beyond:
• Support control inheritance within OSCAL FedRAMP, BOE and XDE
• Support of other templates within OSCAL beyond FedRAMP
• Support the export of control, test, POA&M and risk artifacts within OSCAL
• Support of OSCAL import: profile and SSP layer
Head Start on the OSCAL package for FedRAMP

• What is generated from Xacta360 after an export?
  • Zip file containing FedRAMP SSP in OSCAL format
• What is required in an OSCAL Package for submission to FedRAMP?
  • FedRAMP SSP in OSCAL Format
  • Resolved OSCAL Profile
  • Controls catalog
  • Artifacts in back-matter
Xacta OSCAL Demo
Enable Data Exchange

Enabling Essential Data Exchange in Application Setting

Application Setting Description of EDE

- **Essential Data Exchange** Essential Data Exchange allows master administrators to export projects to Body of Evidence (BOE) XML, (OSCAL) FedRAMP SSP XML, and Xacta Data Exchange (XDE) XML format. Mapping profiles for these formats can be created using the Administration > Application Settings > Essential Data Exchange Mappings page.
Navigate to Project, Select OSCAL Export

Project List Page Action Gear Icon
Can also Select from in Project

**Task List Page “More” Dropdown**

<table>
<thead>
<tr>
<th>Task</th>
<th>Rank</th>
<th>Task Grouping</th>
<th>Task</th>
<th>Approver(s)</th>
<th>Status</th>
<th>Workflow Actions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO GATHERING</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFORMATION SYSTEM POLICIES AND PROCEDURES</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONTINGENCY PLAN</td>
<td>5</td>
<td></td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INCIDENT RESPONSE PLAN</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVACY</td>
<td>15</td>
<td></td>
<td></td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMPLEMENT</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SELF-ASSESSMENT</td>
<td>25</td>
<td></td>
<td></td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OSCAL Located Under Project Tab After Export Message Pops Up

Toaster Message when “Export OSCAL FedRAMP” is selected
<?xml version="1.0" encoding="UTF-8"?>
<system-security-plan xmlns="http://csrc.nist.gov/ns/oscal/1.0" uuid="8872c4a6-2c59-4c02-9d6d-0f07d1">
  <metadata>
    <revisions/>
    <role id="fedramp-jab">=</role>
    <role id="information-system-security-officer">=</role>
    <role id="system-poc-technical">=</role>
    <role id="asset-administrator">=</role>
    <role id="fedramp-pmo">=</role>
    <role id="prepared-by">=</role>
    <role id="authorizing-official">=</role>
  </metadata>

  <system-characteristics>
    <system-id identifier-type="https://fedramp.gov"/>
    <system-name>Information System Name</system-name>
    <system-name-short>System Abbr</system-name-short>
    <description/>
    <prop name="authorization-type" ns="https://fedramp.gov/ns/oscal"/>
    <prop class="security-ecauth" name="security-ecauth-level" ns="https://fedramp.gov/ns/oscal"/>
    <prop name="cloud-service-model"/>
    <prop name="cloud-service-model"/>
  </system-characteristics>
</system-security-plan>
<system-implementation>
  <prop name="users-internal" ns="https://fedramp.gov/ns/oscal" value="test number of internal personnel 500"/>
  <prop name="users-external" ns="https://fedramp.gov/ns/oscal" value="external personnel 40"/>
  <prop name="users-internal-future" ns="https://fedramp.gov/ns/oscal" value="550"/>
  <prop name="users-external-future" ns="https://fedramp.gov/ns/oscal" value="60"/>
  <component type="service" uuid="e3e16dc3-3618-4f17-85cb-c5284b3ba22a"/>
  <component type="this-system" uuid="c94d1b54-a2d0-48fb-b030-ca5493b3b6a7"/>
  <inventory-item uuid="f5a9a920-cd49-4711-b4f0-949cc6941a94"/>
</system-implementation>

<control-implementation>
  <description>
    <implemented-requirement control-id="ma-5" uuid="584669ff-1841-4d1b-83b1-2bda971c0158"/>
    <implemented-requirement control-id="ac-11" uuid="a2d82c3c-e82a-4235-bc9c-04e5e4eca2e3"/>
    <implemented-requirement control-id="ra-5" uuid="d9e13209-a1f1-438c-a26e-7e7ec08dc9b6"/>
    <implemented-requirement control-id="ir-3" uuid="725cffe1-d76b-4214-bbce-ff50e389cbb"/>
    <implemented-requirement control-id="si-3" uuid="1bd7444f-05d8-4330-b02e-f95dccc9b8a5"/>
    <implemented-requirement control-id="ca-2" uuid="389eb03e-0c7a-4407-9232-1ce6c4fba11"/>
  </description>
</control-implementation>
Questions?
For more information on the topics we’ve discussed today:

Visit telos.com/xacta
Contact: sales@telos.com
Solutions that empower and protect the enterprise.