Automating Transition to NIST SP 800-53 Rev. 5 with OSCAL

3rd OSCAL Workshop
March 1, 2022
Welcome! Here’s the Agenda:

• Introduction

• Review of Requirement to Transition to NIST SP 800-53 Rev. 5

• Available OSCAL Tools To Help with Transition

• ATO as a Service™ Workflow to Transition to NIST SP 800-53 Rev. 5

• Q&A
Allow me to re-introduce myself, my name is...

- **Jasson Walker, Jr. CISSP, CPT, CEH, PMP, MCSE**
  - President & CEO of cFocus Software Incorporated
  - 15+ years of experience with FISMA/RMF/FedRAMP compliance

- **cFocus Software Incorporated**
  - Established 2006 with 15+ years of federal IA & cybersecurity experience
  - Providing security compliance for multiple federal agencies (Army, EPA, etc.)
  - [https://cfocussoftware.com](https://cfocussoftware.com)
Introducing ATO as a Service™

• ATO as a Service™ automates FISMA/RMF/FedRAMP compliance and reporting with OSCAL
  ➢ Automates Risk Management Framework process (NIST SP 800-37 Rev. 2)
  ➢ Auto-generates 100% OSCAL v1.0.0 compliant SSPs, POA&Ms, SAPs & SARs
  ➢ Exports authorization package documents to Word/Excel format
Review of Requirement to Transition to NIST SP 800-53 Rev. 5
Requirement to Transition to NIST SP 800-53 Rev. 5

- NIST SP 800-53 Rev. 5 published September 23, 2020
  - Updates published December 10, 2020
- NIST SP 800-53A Rev. 5 published January 25, 2022
- OMB A-130 states, “agencies to comply with NIST standards within one year of publication.”
Automating Transition to NIST SP 800-53 Rev. 5 with OSCAL

Available OSCAL Tools To Help with Transition
Available OSCAL Tools To Help with Transition

- NIST has released NIST SP 800-53 Rev. 5 data in OSCAL format
  - NIST SP 800-53 Rev. 5 = NIST_SP-800-53_rev5_catalog
  - NIST SP 800-53A Rev. 5 = NIST_SP-800-53_rev5_catalog
  - NIST SP 800-53B = NIST_SP-800-53_rev5_LOW-baseline_profile, NIST_SP-800-53_rev5_Moderate-baseline_profile, NIST_SP-800-53_rev5_HIGH-baseline_profile, NIST_SP-800-53_rev5_PRIVACY-baseline_profile
Available OSCAL Tools To Help with Transition

- Furthermore, we can update and extend OSCAL models to incorporate Rev. 4 → Rev. 5 transition data.
- We have extended OSCAL data models in ATO as a Service to include Rev. 5 transition data.

➢ NIST.SP.800-53r4-to-r5 Comparison Workbook
## Available OSCAL Tools To Help with Transition

<table>
<thead>
<tr>
<th>ID</th>
<th>TITLE</th>
<th>Rev 5 Update</th>
<th>NIST SP 800-53 Rev 5 Controls</th>
<th>More than editorial or administrative change? (Y/N)</th>
<th>Changed Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>(Access Control) Policy and Procedures</td>
<td>rev5</td>
<td>NIST SP 800-53 Rev 5 Controls</td>
<td>Y</td>
<td>Changes title, Changes control text, Adds control text, Adds parameter, Changes discussion, Adds to Privacy Control Baseline (SP 800-53)</td>
</tr>
</tbody>
</table>
Available OSCAL Tools To Help with Transition

```json
{
  "name": "rev4-to-rev5-change-major",
  "ns": "https://cfocussoftware.com/ns/oscal",
  "value": "yes"
},
{
  "name": "rev4-to-rev5-change-elements",
  "ns": "https://cfocussoftware.com/ns/oscal",
  "value": [
    "Changes title",
    "Changes control text",
    "Adds control text",
    "Adds parameter",
    "Changes discussion",
    "Adds to Privacy Control Baseline (SP 80-53B)"
  ]
}
```
ATO as a Service™ Workflow to Transition to NIST SP 800-53 Rev. 5
Workflow to Transition to NIST SP 800-53 Rev. 5

- ATO as a Service™ utilizes OSCAL to automate the transition from NIST SP 800-53 Rev 4 to Rev. 5
Workflow to Transition to NIST SP 800-53 Rev. 5

• Step 1: Create custom converter from .doc/docx/.xls/.xlsx → OSCAL SSP file
• Step 2: Establish common controls, components & organization-defined values
• Step 3: Verify System Categorization & Security Control Selection
Workflow to Transition to NIST SP 800-53 Rev. 5

• **Step 4: Automatically mark as compliant all security controls with minor changes**
  - 491 NIST SP 800-53 Rev. 5 security controls (including withdrawn controls) have only minor changes

• **Step 5: Evaluate each security control with major changes**

• **Step 6: Decide to implement control or auto-generate POA&M**

Automating Transition to NIST SP 800-53 Rev. 5 with OSCAL
Q&A
Thank you! Any Questions?

• Let’s keep in touch! Here’s my contact Info:
  ➢ Jasson Walker, Jr.
  ➢ jasson.walker@cfocussoftware.com
  ➢ (301) 499-2650 office
  ➢ (301) 455-4030 mobile
  ➢ https://cfocussoftware.com