Shifting Left the Right Way with OSCAL

A Case Study using the Open Security Controls Assessment Language

Chris Compton, Alexander Stein, Nikita Wootten
Information Technology Laboratory
Computer Security Division
Case Study
Managing Risk With OSCAL

A research pilot for secure information exchange between multiple organizations that is continuously monitored, assessed and authorized to operate.
Case Study
The Question

Controls

SP 800-53
Catalog of Security and Privacy Controls for Information Systems and Organizations

Process

RMF
Risk Management Framework

nist.gov/rmf
OSCAL
Open Security Controls Assessment Language

- Open Source Project on GitHub
- First Official Release: June 7, 2021
Produce and interpret **machine-readable security documentation** using a common specification that promotes interoperability.
OSCAL Overview
Open Security Controls Assessment Language

Documentation At Scale
GRC TOOLS AND SERVICES
SECURITY DOCUMENTS
Enables **automated traceability** from selection of security controls through implementation and assessment.
OSCAL Overview

Open Security Controls Assessment Language

Models in Development: Control Mapping, Shared Responsibility

https://pages.nist.gov/OSCAL/
Certain products may be identified on this web page, but such identification does not imply recommendation by the US National Institute of Standards and Technology or other agencies of the US Government, nor does it imply that the products identified are necessarily the best available for the purpose.
Give OSCAL a Try!
Not Just for Government...

Also: Get Involved!

- Past OSCAL Workshops
- Reference Documentation
- Community Teleconferences
- Future “Office Hours”

- Contributions of Code, Experiences and Expertise!

https://pages.nist.gov/OSCAL/contribute/

Members of the Army’s parachute demonstration team, the Golden Knights, give each other a high five before jumping from an aircraft over Hazel Green, Wis., July 2, 2022. - Defense.gov Photo
Workflow
How do we participate earlier in the development process, with constructive feedback, and documentation that contributes to the momentum of the project?
GitHub Workflow
.github/workflows.ci.yaml

Application Unit Testing → All OSCAL Model Content → OSCAL Assessment Plan → OSCAL Assessment Result

- CUSTOM ACTION: OSCAL Validation
  .github/actions/oscal-validation

- CUSTOM ACTION: OSCAL Assessment
  .github/actions/oscal-assess

- CUSTOM ACTION: OSCAL Validation
  .github/actions/oscal-validation

- OSCAL Profile + Full Catalog
  Execute Plan Tasks
  Findings Comment Added to Pull Request

- Profile Resolution
  Result Generation

- OSCAL Catalog
  OSCAL Assessment Result
AC-8 System Use Notification

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;

[...SNIP...]
NIST 800-53
Over 1100 Controls and Enhancements
**Development + Security**

**Documenting: System Security Plans**

### OSCAL System Security Plan

<table>
<thead>
<tr>
<th>AC-8</th>
<th>Control Summary Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Role:</td>
<td></td>
</tr>
<tr>
<td>Parameter AC-8(a):</td>
<td></td>
</tr>
<tr>
<td>Parameter AC-8(c): 1:</td>
<td></td>
</tr>
<tr>
<td>Implementation Status (check all that apply):</td>
<td></td>
</tr>
<tr>
<td>- Implemented</td>
<td></td>
</tr>
<tr>
<td>- Partially Implemented</td>
<td></td>
</tr>
<tr>
<td>- Planned</td>
<td></td>
</tr>
<tr>
<td>- Alternative implementation</td>
<td></td>
</tr>
<tr>
<td>- Not applicable</td>
<td></td>
</tr>
<tr>
<td>Control Origin (check all that apply):</td>
<td></td>
</tr>
<tr>
<td>- Service Provider Corporate</td>
<td></td>
</tr>
<tr>
<td>- Service Provider System Specific</td>
<td></td>
</tr>
<tr>
<td>- Service Provider Hybrid (Corporate and System Specific)</td>
<td></td>
</tr>
<tr>
<td>- Configured by Customer (Customer System Specific)</td>
<td></td>
</tr>
<tr>
<td>- Provided by Customer (Customer System Specific)</td>
<td></td>
</tr>
<tr>
<td>- Shared (Service Provider and Customer Responsibility)</td>
<td></td>
</tr>
<tr>
<td>- Invented from pre-existing FedRAMP Authorization for Click here to enter text, Date of Authorization</td>
<td></td>
</tr>
</tbody>
</table>

**The ‘Old’ Way**

You are accessing a U.S. Government information system, which includes: 1) all Government-furnished computers connected to this network, and 2) all media attached to this network or to a computer on this network. You understand may access this information system for authorized use only; unauthorized access to criminal and civil penalties; you have no reasonable expectation of privacy when transiting or stored on this information system at any time and for any purpose. This system monitors, intercepts, and searches any communication or data and any communications or data transiting or stored on this information system in accordance with law, regulations, and Government purpose. This information system may contain Controlled Unclassified information and may be monitored to safeguarding or dissemination controls in accordance with law, regulations, or Government purpose. Using this system indicates your understanding of this warning.

**Statements**

- statement-id: ac-8_smt.a
  - uid: 6f6b8993-2f85-468c-95f7-8f1fe4657f16
  - by-components:
    - component-uid: 413c1ce-92dc-494b-82e0-889618597da
      - uid: 59a5d037-1154-499f-8401-c86e4a0b5378
      - description: The system use notification will be implemented in the following locations:
        - Server log in
        - Application log in
      - props:
        - name: responsibility
        - value: provider

**Traditional Document**
**Development + Security**

**Automated Assessment Plan**

```python
27 tasks:
28   - uuid: 6b7e6a29-4588-46be-b242-a0b8a40f20de
29     title: Validate System Use Notification Presence from Python Script
30     description: Check system use notification presence.
31     type: action
32     props:
33       - name: ar-check-method
34         ns: https://www.nist.gov/itl/csd/ssag/blossom
35         value: system-shell-return-code
36       - name: ar-check-result
37         ns: https://www.nist.gov/itl/csd/ssag/blossom
38         value: "0"
```

---

**Developer Change**

**Software Testing**

**OSCAL Content Validation**

**Assessment Plan Execution**

---

**GitHub Actions**

- **application_test**: 1m 6s
- **oscal_validate**: 32s
- **oscal_assess**: 39s
Demonstration
Questions?

Contact Us!
oscal@nist.gov

https://pages.nist.gov/OSCAL/
https://github.com/usnistgov/blossom-case-study

GitHub Case Study Project

Chris Compton, Alexander Stein, Nikita Wootten
Information Technology Laboratory
Computer Security Division