

Shifting Left the Right Way with OSCAL

A Case Study using the Open Security Controls Assessment Language

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



?

OSCAL

Open Security Controls Assessment Language

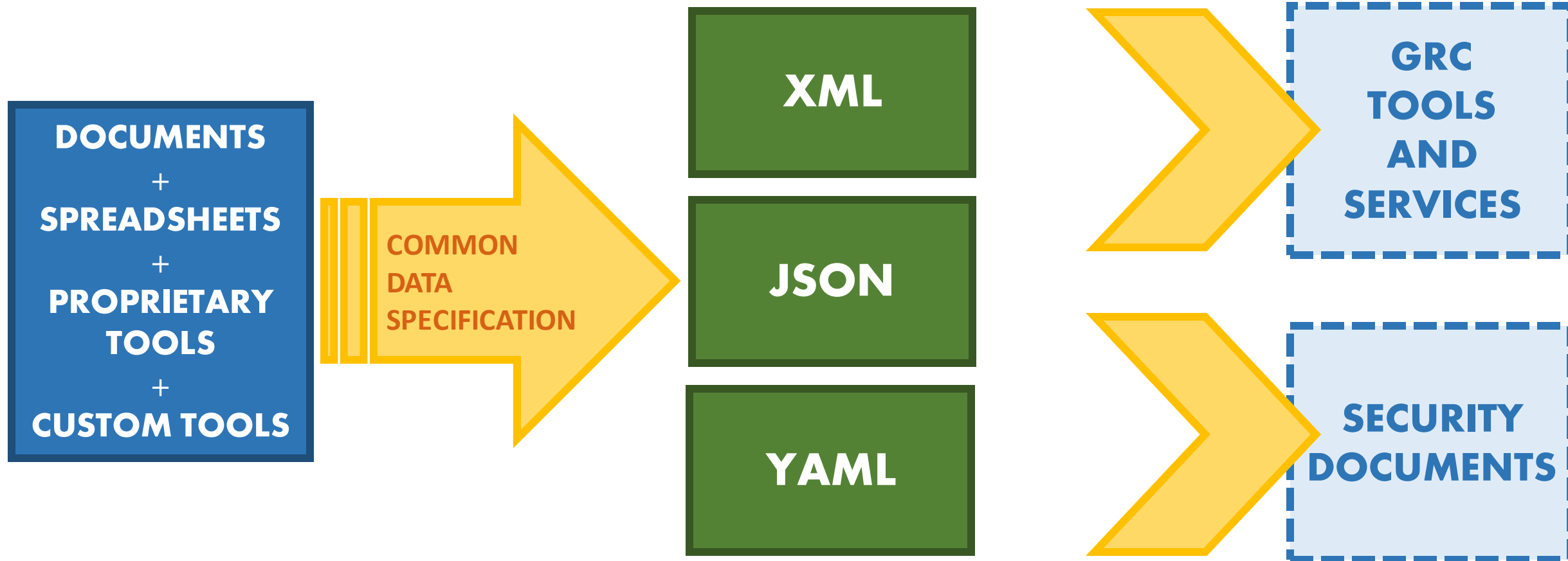
- Open Source Project on GitHub
- First Official Release: June 7, 2021

Produce and interpret **machine-readable security documentation** using a common specification that promotes interoperability.

OSCAL Overview


Open Security Controls Assessment Language

Documentation At Scale



OSCAL Overview

Open Security Controls Assessment Language



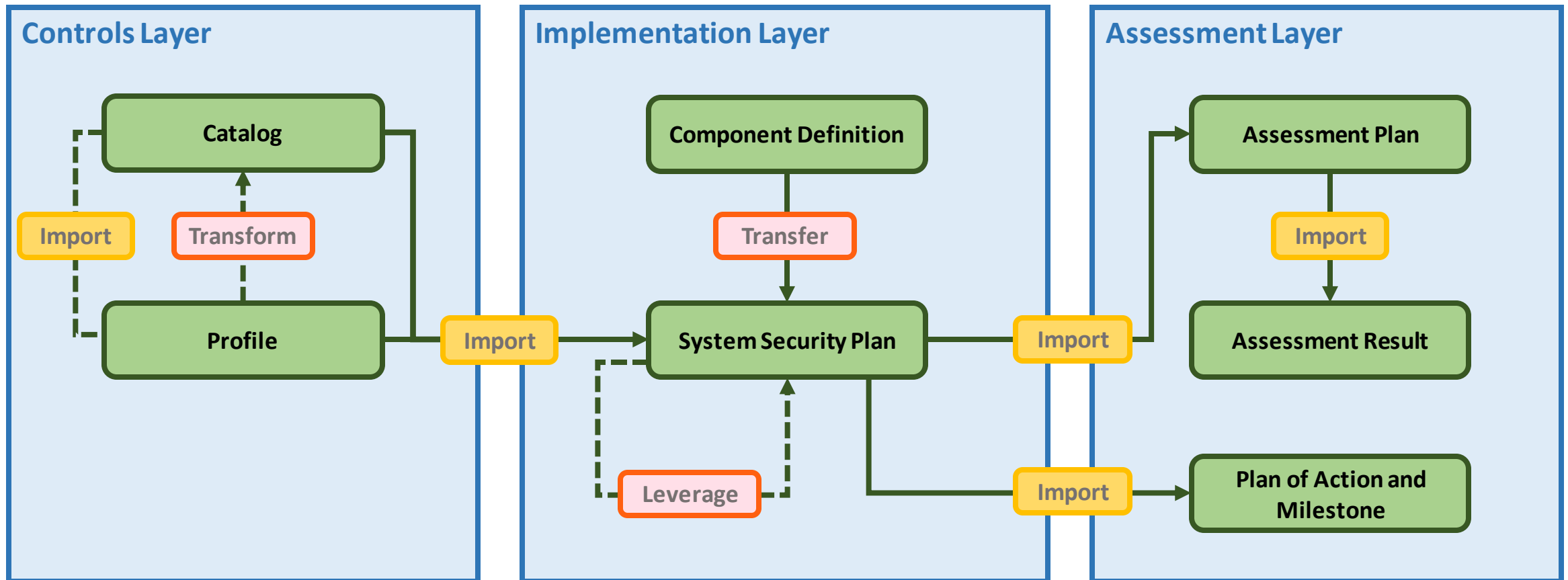
Enables **automated traceability** from selection of security controls through implementation and assessment.

OSCAL Overview

Open Security Controls Assessment Language

Information Flow

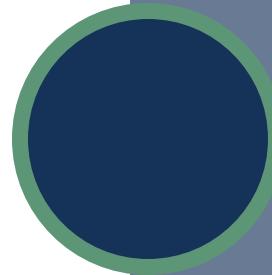
Traceability



OSCAL Tools

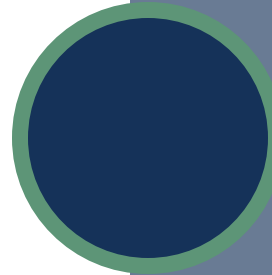
<https://pages.nist.gov/OSCAL/tools/>

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.



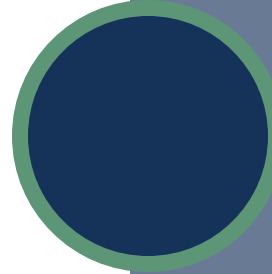
Model Validation

NIST OSCAL-CLI



Conversion & Resolution

NIST OSCAL-CLI | XML, JSON, YAML



Open Source and Commercial License Tools

Give OSCAL a Try!

Not Just for Government...



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

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/>

Workflow

Development + Security

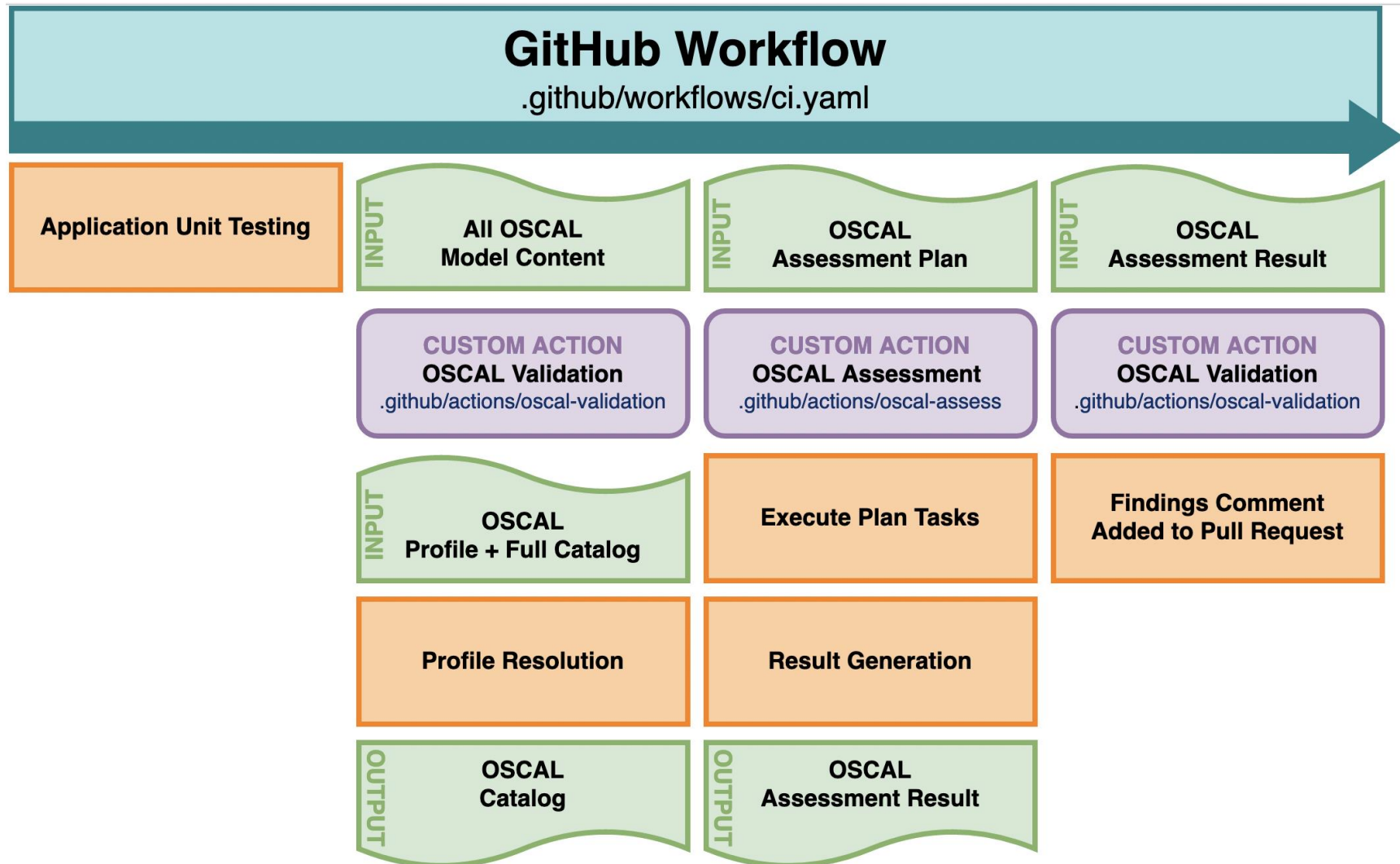
Documenting Practices, Standards and Process



How do we **participate earlier in the development process**, with constructive feedback, and documentation that contributes to the momentum of the project?

Development + Security

Big Picture View of the Workflow



Development + Security

Documenting Practices, Standards and Process

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...]

Development + Security

Documenting: Catalogs of Controls

NIST 800-53
Over **1100** Controls
and Enhancements

```
33     - role-id: contact
34     party-uuids:
35         - 33434b58-3a4b-4a4f-a490-e7369c068847
36     imports:
37         - href: https://raw.githubusercontent.com/usnist
38     include-controls:
39         - with-ids:
            - ac-8
```

OSCAL Profile

```
15     groups:
16     - id: ac
17       class: family
18       title: Access Control
19       controls:
20       - id: ac-8
21         class: SP800-53
22         title: System Use Notification
23         params:
24         - id: ac-08_odp.01
25           label: system use notification
26           guidelines:
27             - prose: system use notification message o
28         - id: ac-08_odp.02
29           label: conditions
30           guidelines:
31             - prose: conditions for system use to be d
```

OSCAL Resolved Catalog

Development + Security

Documenting: System Security Plans

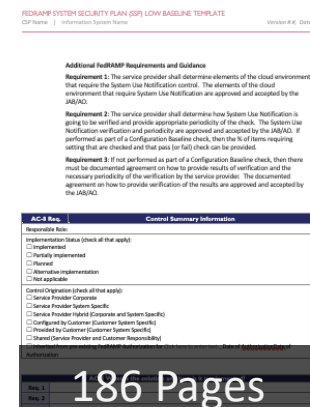
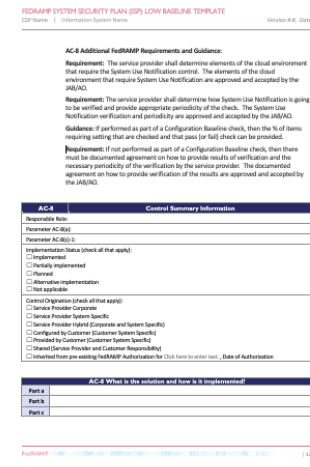
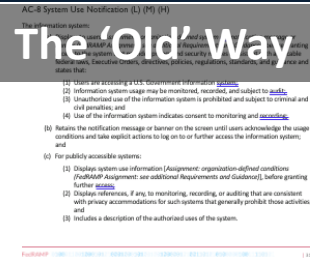
OSCAL System Security Plan

```
71 control-implementation:
72   description: This system implements a very minimal set of controls for demonstration only.
73   implemented-requirements:
74     - uuid: 83f12e58-3091-4dc6-a26b-391fb7b0fb40
75       control-id: ac-8
76       set-parameters:
77         - param-id: ac-8_prm_1
78           values:
79             - >-
80             You are accessing a U.S. Government information system, which includes: 1
81             3) all Government-furnished computers connected to this network, and 4) a
82             media attached to this network or to a computer on this network. You unde
83             may access this information system for authorized use only; unauthorized
84             to criminal and civil penalties; you have no reasonable expectation of pr
85             transiting or stored on this information system at any time and for any l
86             monitor, intercept, audit, and search and seize any communication or data
87             and any communications or data transiting or stored on this information s
88             Government purpose. This information system may contain Controlled Unclas
89             safeguarding or dissemination controls in accordance with law, regulation
90             using this system indicates your understanding of this warning.
91   statements:
92     - statement-id: ac-8_smt.a
93       uuid: 6f668993-2f85-4e8c-95ff-0f1fe4657f16
94       by-components:
95         - component-uuid: a413cc1e-92dc-494b-b2ed-a8d9610597da
96           uuid: a59a5d37-1154-4997-b4d1-c06e4ab53707
97           description: >-
98           The system use notification will be implemented in the following locati
99           * Server log in
100          * Application log in
101       props:
102         - name: responsibility
103           value: provider
```

Traditional Document

AC-8	Control Summary Information
Responsible Role:	
Parameter AC-8(a):	
Parameter AC-8(c)-1:	
Implementation Status (check all that apply): <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	
Control Origination (check all that apply): <input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-8 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	



Development + Security

Automated Assessment Plan

Developer Change

Software Testing

OSCAL Content Validation

Assessment Plan Execution

```
27 tasks:
28   - uuid: 6b7e6a29-4588-46be-b242-a0bda0092e2c
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"
```

OSCAL Assessment Plan

ci.yaml
on: pull_request

✓ application_test 1m 6s

✓ oscal_validate 32s

✓ oscal_assess 39s

GitHub Actions

Demonstration

Questions?

GitHub Case Study Project

Contact Us!




oscal@nist.gov


<https://pages.nist.gov/OSCAL/>

<https://github.com/usnistgov/blossom-case-study>



Appendix: The Demo App

 96e25753a1  10 branches  0 tags Go to file <> Code

 nikitawootten-nist Added the demonstration application ✓ 96e2575 16 hours ago 🕒 2 commits

📁 .github/workflows	Al <code>import os</code>
📁 app	Al <code>from fastapi import FastAPI, Request</code> <code>from fastapi.templating import Jinja2Templates</code>
📁 cypress	Al <code>from pathlib import Path</code>
📁 tests	Al <code># the "app" directory</code> <code>base_path = Path(__file__).parent</code>
📄 .gitignore	Al
📄 README.md	Sl <code>description = base_path.joinpath('README.md').read_text(encoding='utf-8')</code> <code>enroller = FastAPI(</code>
📄 cypress.config.js	Al <code>title="Government Agency",</code> <code>description=description,</code> <code>version="0.0.1"</code>
📄 docker-compose.yml	Al <code>)</code>
📄 package-lock.json	Al <code>templates = None</code>
📄 package.json	Al <code>views_path = base_path.joinpath('views')</code> <code>if os.path.exists(views_path):</code>
📄 requirements.txt	Al <code>views = Jinja2Templates(directory=views_path)</code> <code>else:</code>
📄 run.sh	Al <code>raise Exception("Could not find Views directory. Expecting 'views/'.")</code> <code>@enroller.get("/")</code> <code>async def read_root(request: Request):</code> <code>return views.TemplateResponse("warning/non_conforming.html", { "request": request })</code>

Welcome to the application!

Enjoy your stay!

[Main](#) | [Documentation](#)



NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Appendix: Automated Assessment


tasks:

- **uuid:** 6b7e6a29-4588-46be-b242-a0bda0092eec
 - title:** Validate System Use Notification Presence from Python Script
 - description:** Check system use notification presence.
 - type:** action
 - associated-activities:**
 - **activity-uuid:** d85636e6-0d9d-4c94-a924-5a612a119040
 - subjects:**
 - **type:** component
 - include-all:** {}
 - props:**
 - **name:** ar-check-method
 - ns:** <https://www.nist.gov/itl/csd/ssag/blossom>
 - value:** system-shell-return-code
 - **name:** ar-check-result
 - ns:** <https://www.nist.gov/itl/csd/ssag/blossom>
 - value:** "0"

```
1  #!/usr/bin/env python3
2  # Consumed by the oscal-workflow harness
3
4  import os
5  import textwrap
6  from urllib import request
7
8  from bs4 import BeautifulSoup
9
10 # The system use notification text
11 expected_use_notification = os.getenv('SSP_PARAM_AC_8_PRM_1')
12 if expected_use_notification is None:
13     raise Exception('ac-8_prm_1 must be defined in the SSP')
14
15 # running via docker-compose.yaml
16 response = request.urlopen('http://127.0.0.1:10000')
17
18 soup = BeautifulSoup(response, 'html.parser')
19
20 # Drill into the element that the system use notification text lives
21 raw_use_notification = soup.body.div.p.text
22 clean_use_notification = textwrap.dedent(raw_use_notification).strip().replace('\n', ' ')
23
24 assert clean_use_notification == expected_use_notification
```


Appendix: Bringing the System Into Compliance

Triggered via pull request 16 hours ago

 nikitawootten-nist opened #28 [step_3](#)

Status

Total duration

Billable time

Artifacts

Failure

1m 58s

4m

1

ci.yaml

on: pull_request

application_test

11s

oscal_validate

38s

oscal_assess

1m 1s

Annotations


1 error

oscal_assess


Process completed with exit code 1.

Artifacts

Produced during runtime

Name	Size
 assessment-results	2.57 KB

1 comment on commit d1ce23a

 github-actions bot commented on d1ce23a 16 hours ago

OSCAL Workflow Automated Assessment Results

Assessment Results for Testing of SYSTEM

Observation Title	Target	Status
Validate System Use Notification Presence from Python Script	ac-8_obj.a.1	<div>✖ (reason: failed)</div>

For more details, check the artifacts for this commit for an assessment results document.

```
24 @enroller.get("/")
25 async def read_root(request: Request):
-     return views.TemplateResponse("warning/non_conforming.html", { "request": request })
26 +     return views.TemplateResponse("warning/conforming.html", { "request": request })
```