Shifting Left the Right Way with OSCAL

A Case Study using the Open Security Controls Assessment Language

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

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

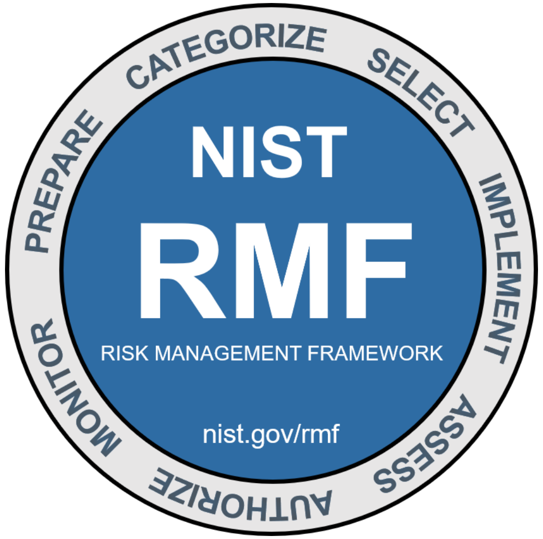
SP 800-53

Catalog of Security and Privacy Controls for Information Systems and Organizations

Process

RMF

Risk Management Framework



?

OSCAL

Open Security Controls Assessment Language

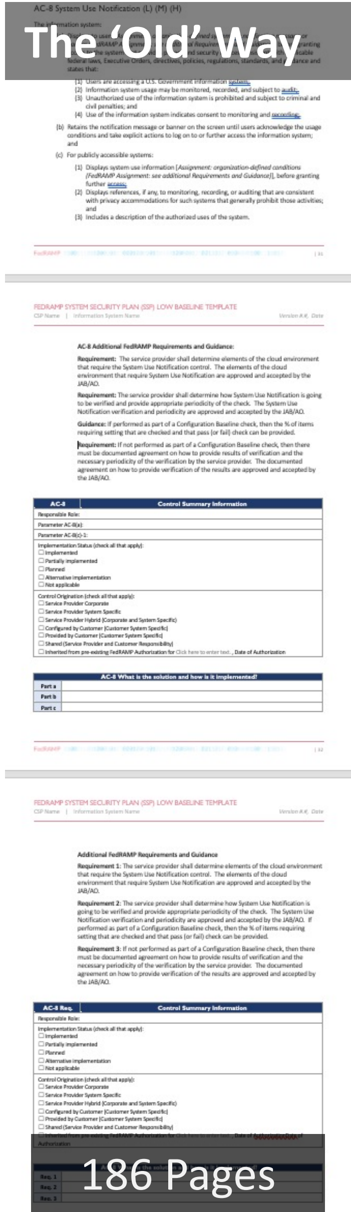
- Open Source Project on GitHub
- First Official Release: June 7, 2021

OSCAL Overview

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

Open Security Controls Assessment Language

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



The 'Old' Way

AC-8 System Use Notification (L) (M) (H)

The information system:

(a) Displays to users [illegible] federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

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

(b) Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

(c) For publicly accessible systems:

(1) Displays system use information [*Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)*], before granting further access;
(2) Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
(3) Includes a description of the authorized uses of the system.

FedRAMP | 31

FEDRAMP SYSTEM SECURITY PLAN (SSP) LOW BASELINE TEMPLATE
CSP Name | Information System Name Version #.#, Date

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

AC-8	Control Summary Information
Responsible Role:	
Parameter AC-8(a):	
Parameter AC-8(c)-1:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ 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	

FedRAMP | 32

FEDRAMP SYSTEM SECURITY PLAN (SSP) LOW BASELINE TEMPLATE
CSP Name | Information System Name Version #.#, Date

Additional FedRAMP Requirements and Guidance

Requirement 1: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement 2: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement 3: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

AC-8 Req.	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ 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?	
Req. 1	
Req. 2	
Req. 3	

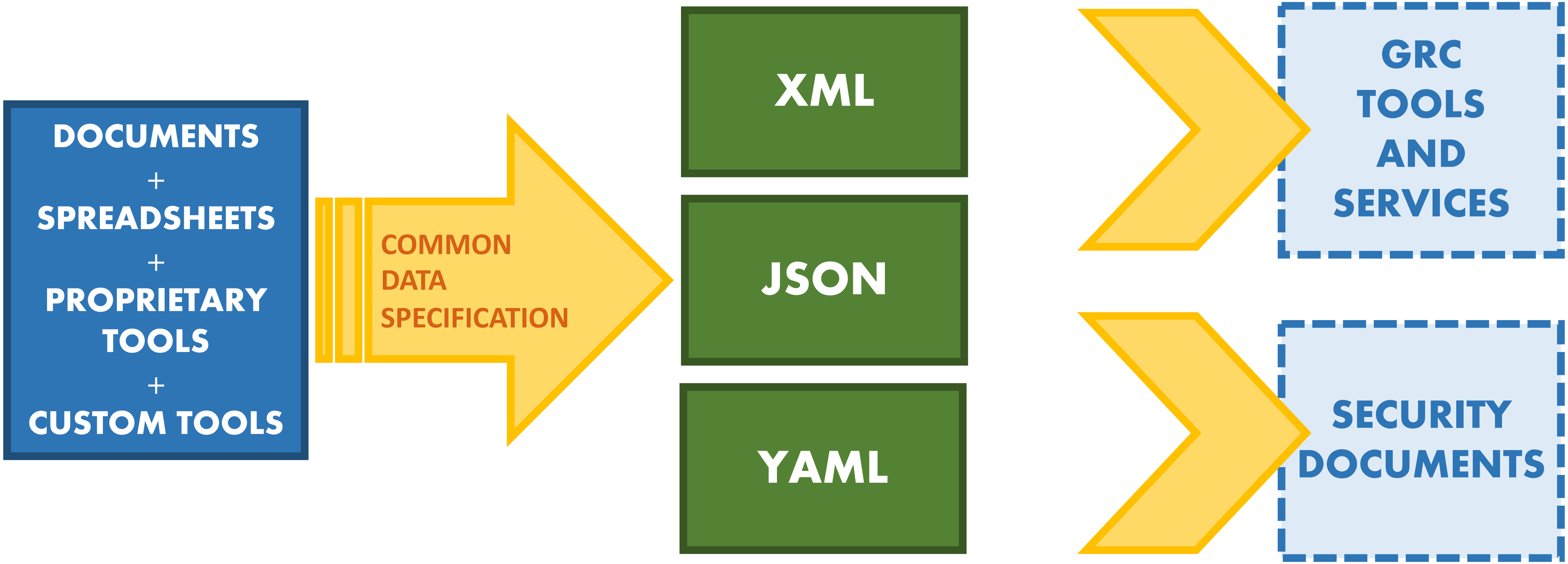
186 Pages

OSCAL Overview

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

Open Security Controls Assessment Language

Documentation At Scale



DOCUMENTS
+
SPREADSHEETS
+
PROPRIETARY TOOLS
+
CUSTOM TOOLS

COMMON DATA SPECIFICATION

XML

JSON

YAML

GRC TOOLS AND SERVICES

SECURITY DOCUMENTS

OSCAL Overview

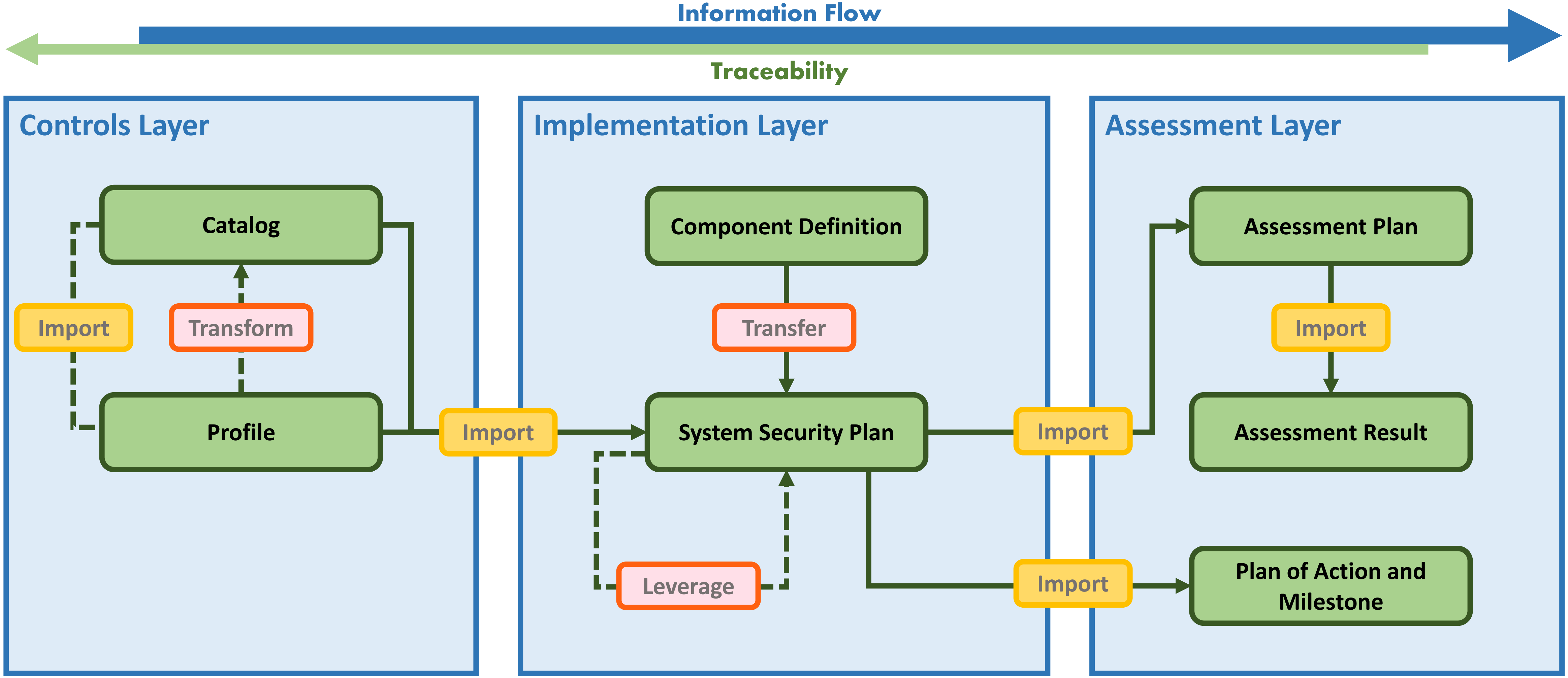
Open Security Controls Assessment Language

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

OSCAL Overview

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

Open Security Controls Assessment Language



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

Models in Development: Control Mapping, Shared Responsibility

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

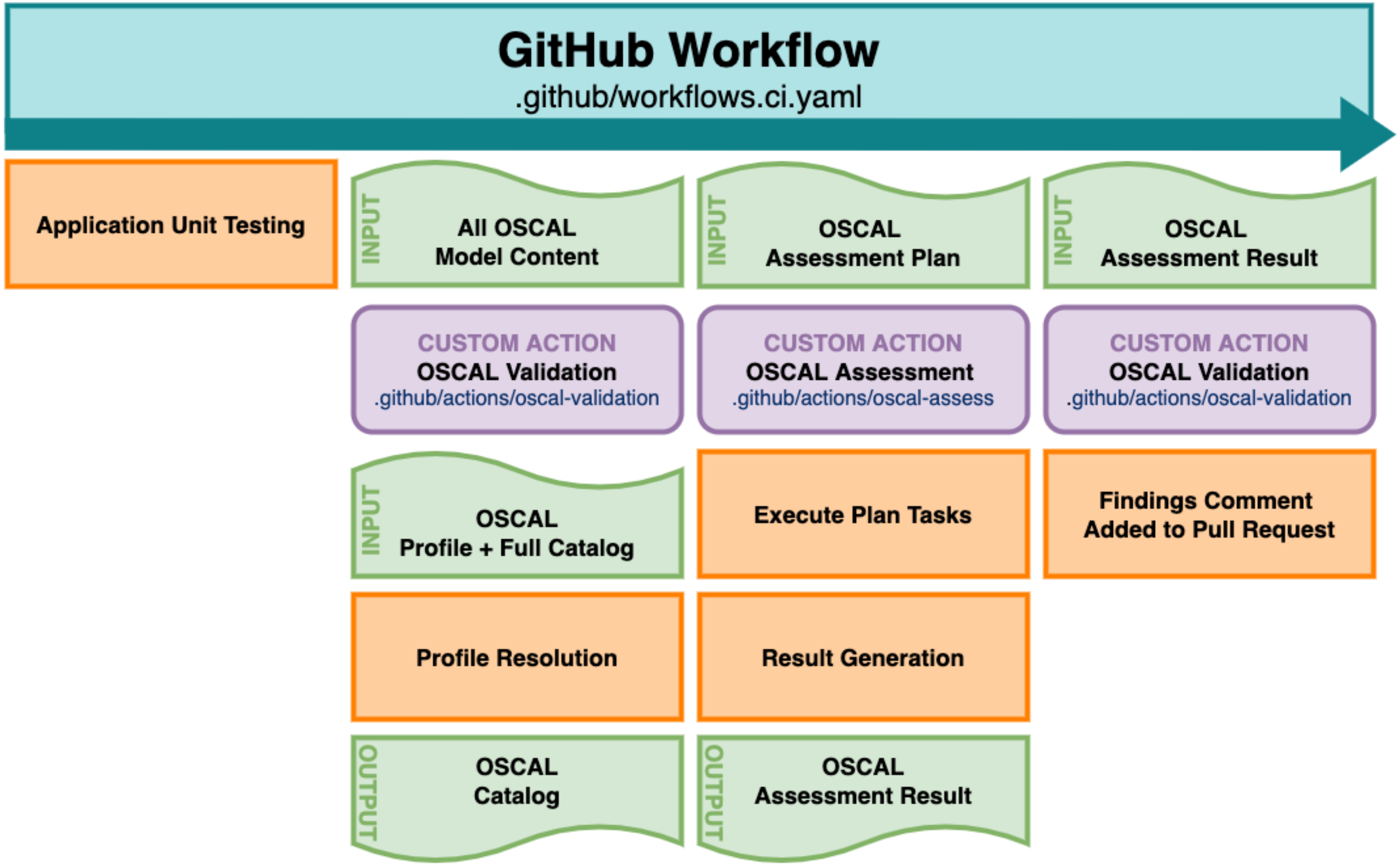
How do we **participate earlier in the development process**, with constructive feedback, and documentation that contributes to the momentum of the project?

Hand off to Nikita

Development + Security

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

Big Picture View of the Workflow



GitHub Workflow

.github/workflows.ci.yaml

Application Unit Testing

INPUT: All OSCAL Model Content

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

INPUT: OSCAL Profile + Full Catalog

Profile Resolution

OUTPUT: OSCAL Catalog

INPUT: OSCAL Assessment Plan

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

Execute Plan Tasks

Result Generation

OUTPUT: OSCAL Assessment Result

INPUT: OSCAL Assessment Result

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

Findings Comment Added to Pull Request

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;

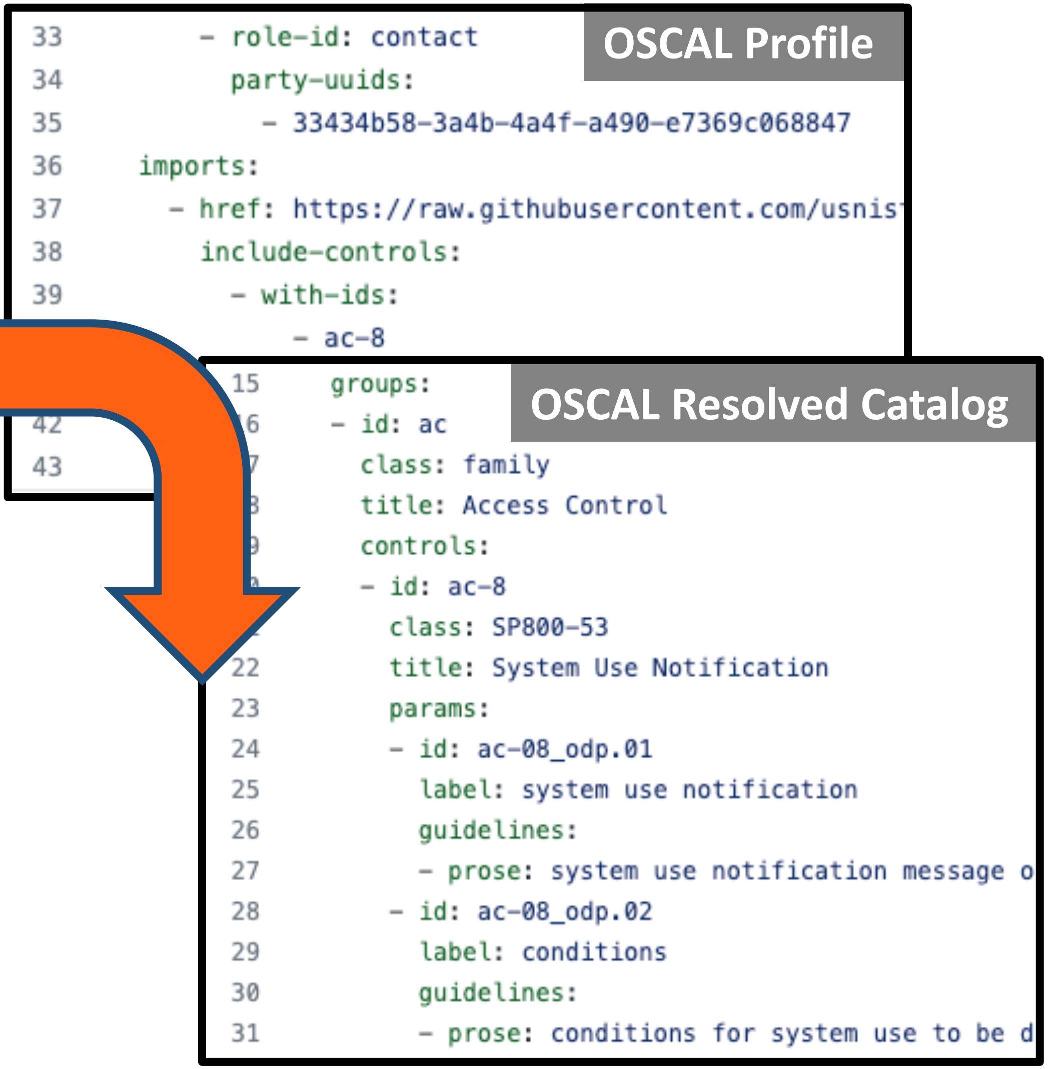
[...SNIP...]

Development + Security

Documenting: Catalogs of Controls

NIST 800-53

Over **1100** Controls and Enhancements



OSCAL Profile

```
      - role-id: contact
        party-uuids:
          - 33434b58-3a4b-4a4f-a490-e7369c068847
  imports:
    - href: https://raw.githubusercontent.com/usnis
      include-controls:
        - with-ids:
            - ac-8
```

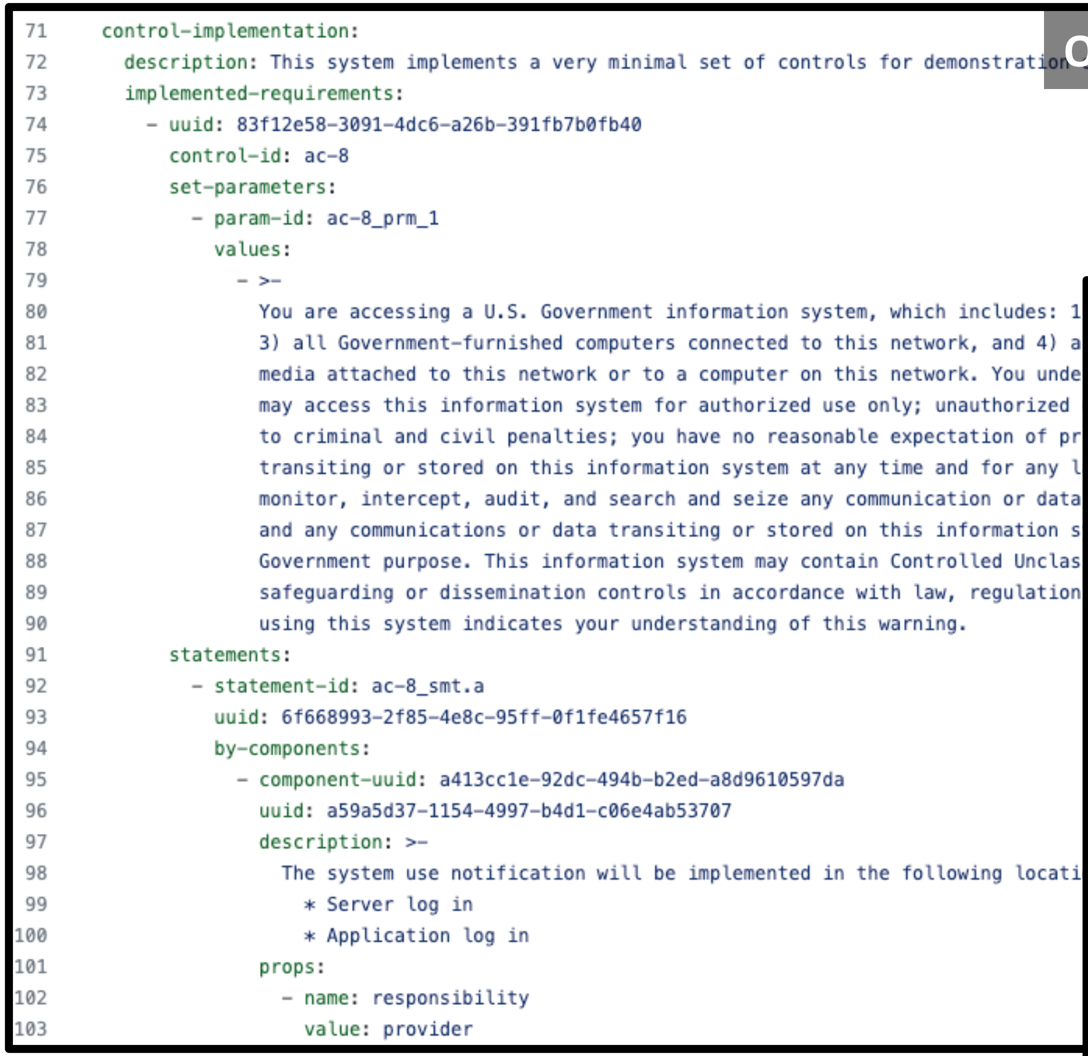
OSCAL Resolved Catalog

```
    groups:
      - id: ac
        class: family
        title: Access Control
        controls:
          - id: ac-8
            class: SP800-53
            title: System Use Notification
            params:
              - id: ac-08_odp.01
                label: system use notification
                guidelines:
                  - prose: system use notification message o
              - id: ac-08_odp.02
                label: conditions
                guidelines:
                  - prose: conditions for system use to be d
```

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

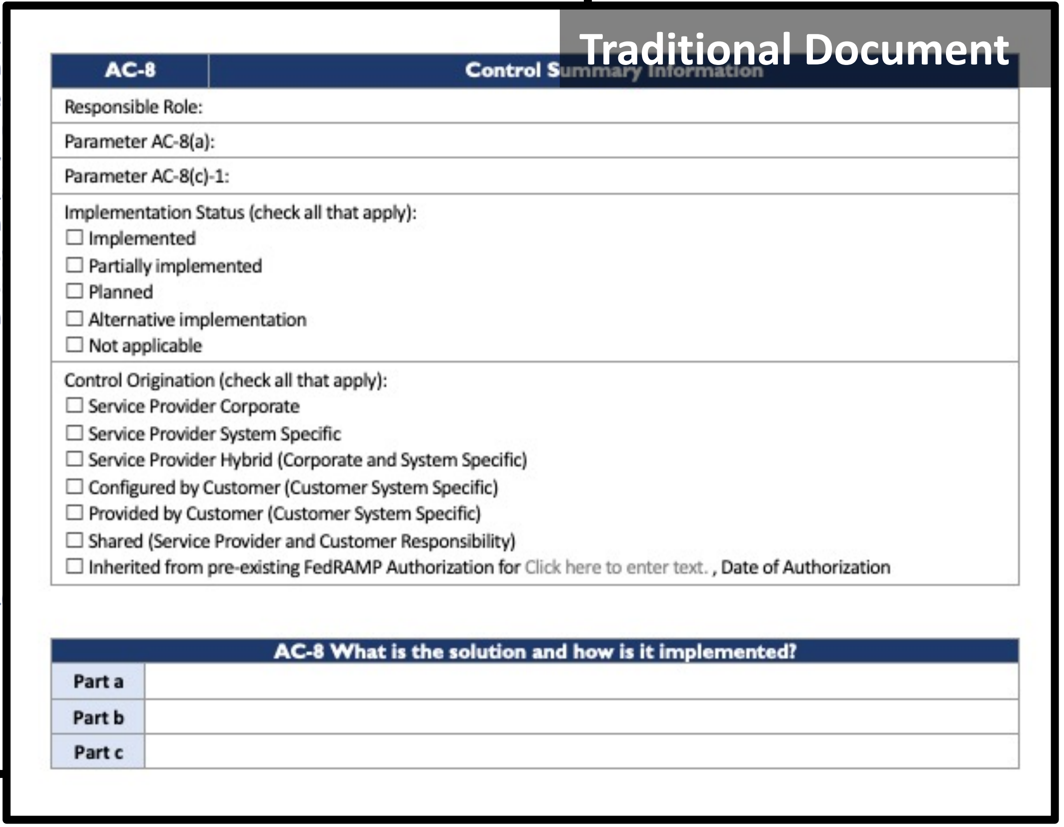
Development + Security

Documenting: System Security Plans



OSCAL System Security Plan

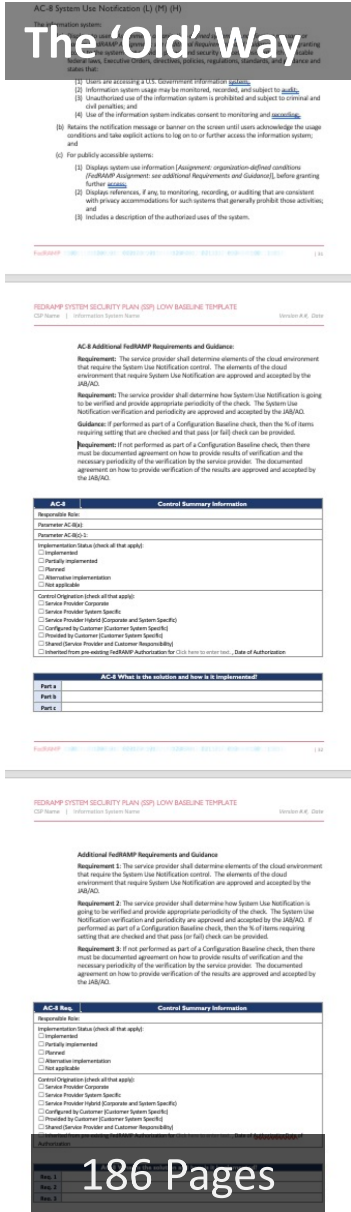
```
control-implementation:
  description: This system implements a very minimal set of controls for demonstration
  implemented-requirements:
    - uuid: 83f12e58-3091-4dc6-a26b-391fb7b0fb40
      control-id: ac-8
      set-parameters:
        - param-id: ac-8_prm_1
          values:
            - >-
              You are accessing a U.S. Government information system, which includes: 1
              3) all Government-furnished computers connected to this network, and 4) a
              media attached to this network or to a computer on this network. You unde
              may access this information system for authorized use only; unauthorized
              to criminal and civil penalties; you have no reasonable expectation of pr
              transiting or stored on this information system at any time and for any l
              monitor, intercept, audit, and search and seize any communication or data
              and any communications or data transiting or stored on this information s
              Government purpose. This information system may contain Controlled Unclas
              safeguarding or dissemination controls in accordance with law, regulation
              using this system indicates your understanding of this warning.
      statements:
        - statement-id: ac-8_smt.a
          uuid: 6f668993-2f85-4e8c-95ff-0f1fe4657f16
          by-components:
            - component-uuid: a413cc1e-92dc-494b-b2ed-a8d9610597da
              uuid: a59a5d37-1154-4997-b4d1-c06e4ab53707
              description: >-
                The system use notification will be implemented in the following locati
                  * Server log in
                  * Application log in
              props:
                - name: responsibility
                  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): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ 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	

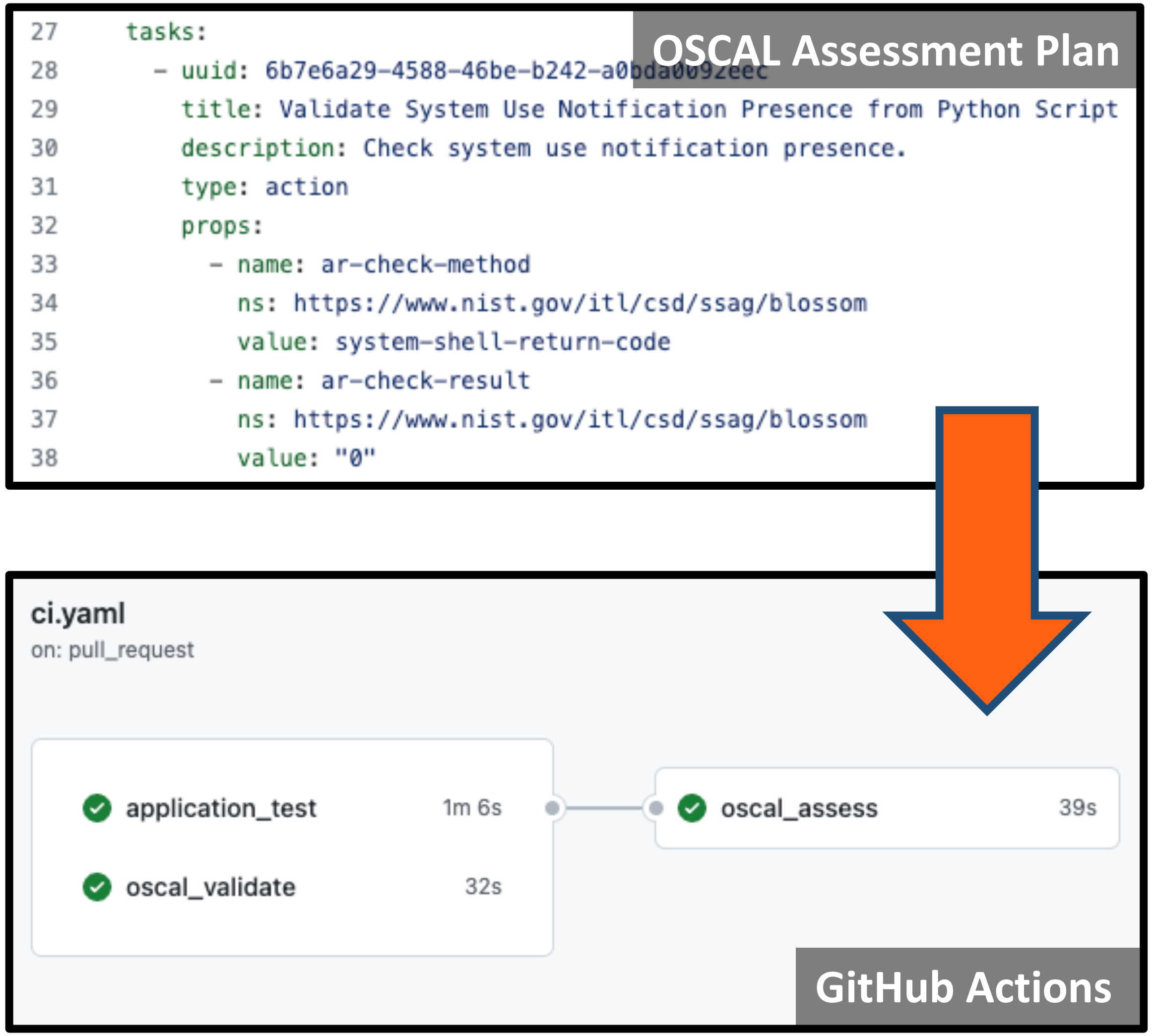


The 'Old' Way

186 Pages

Development + Security

Automated Assessment Plan



OSCAL Assessment Plan

```yaml
  tasks:
    - uuid: 6b7e6a29-4588-46be-b242-a0bda0092eec
      title: Validate System Use Notification Presence from Python Script
      description: Check system use notification presence.
      type: action
      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"
```

ci.yaml

on: pull_request

GitHub Actions

Developer Change

Software Testing

OSCAL Content Validation

Assessment Plan Execution

Case Study

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

Demonstration

Questions?

GitHub Case Study Project

Contact Us!

oscal@nist.gov

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

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

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