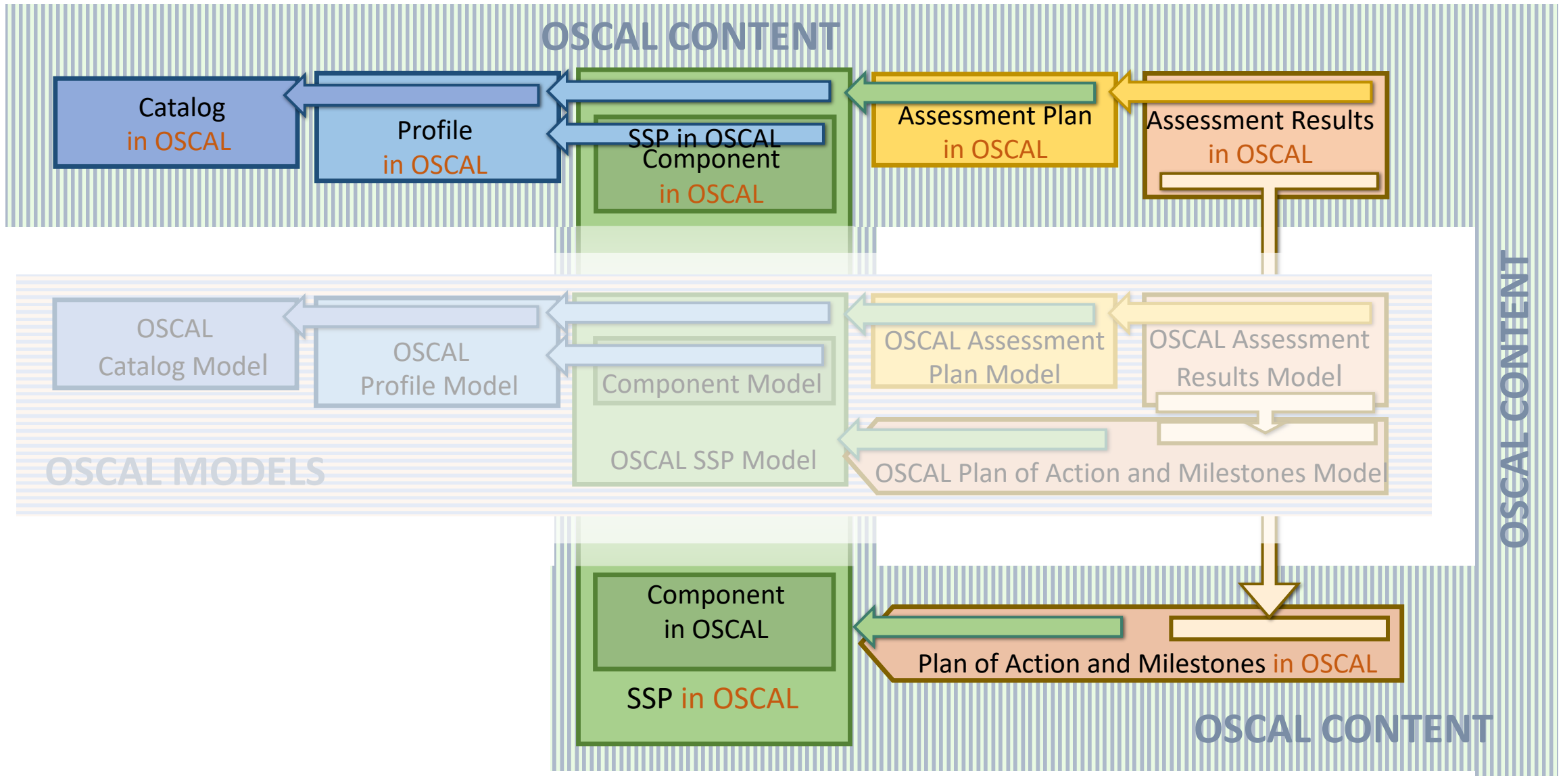
OSCAL Content

February 2, 2021

National Institute of Standards and Technology
U.S. Department of Commerce

What is OSCAL Content?



NIST OSCAL (XML, JSON, YAML) Catalogs and Profiles

https://github.com/usnistgov/oscal-content

Maintainer	OSCAL Information		Source Documents
NIST	SP 800-53 Catalog	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 NIST Low Baseline	Rev 4	NIST SP 800-53 Rev4
	SP 800-53 NIST Moderate Baseline	Rev 4	NIST SP 800-53 Rev4
	SP 800-53 NIST High Baseline	Rev 4	NIST SP 800-53 Rev4
	SP 800-53 NIST Resolved Low Baseline	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 NIST Resolved Moderate Baseline	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 NIST Resolved High Baseline	Rev 4	NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4
	SP 800-53 Catalog	Rev 5	NIST SP 800-53 Rev5
	SP 800-53 NIST Low Baseline	Rev 5	NIST SP 800-53 Rev5B
	SP 800-53 NIST Moderate Baseline	Rev 5	NIST SP 800-53 Rev5B
	SP 800-53 NIST High Baseline	Rev 5	NIST SP 800-53 Rev5B
	SP 800-53 NIST Privacy Baseline	Rev 5	NIST SP 800-53 Rev5B
FedRAMP	SP 800-53 FedRAMP Low Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Moderate Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP High Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Tailored Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Low Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Moderate Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved High Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Tailored Baseline	Rev 4	FedRAMP Security Controls Baselines

- examples
- fedramp.gov
- nist.gov/SP800-53
- oscal @ d26e3b3
- src

OSCAL (XML, JSON, YAML) Examples

https://github.com/usnistgov/oscal-content

- examples
- fedramp.gov
- nist.gov/SP800-53
- oscal @ d26e3b3
- src

- The contents of the examples directory are as follows:
  - catalog: This directory contains sample content for the OSCAL catalog model.
  - component-definition: This directory contains sample content for the OSCAL component definition model.
  - ssp: This directory contains sample content for the OSCAL system security plan (SSP) model.
- Not real data

FedRAMP OSCAL (XML, JSON and YAML) Profiles

https://github.com/GSA/fedramp-automation:

- assets
- baselines
- documents
- oscal @ 5581a8e
- resources
- src
- templates

Maintainer	OSCAL Information		Source Documents
FedRAMP	SP 800-53 FedRAMP Low Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Moderate Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP High Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Tailored Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Low Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Moderate Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved High Baseline	Rev 4	FedRAMP Security Controls Baselines
	SP 800-53 FedRAMP Resolved Tailored Baseline	Rev 4	FedRAMP Security Controls Baselines

EXAMPLE 1: OSCAL CATALOG CONTENT

THE SP800-53R5 AC-5 CONTROL (PROSE)

AC-5 SEPARATION OF DUTIES

Control:

a. Identify and document [*Assignment: organization-defined duties of individuals requiring separation*]; and

b. Define system access authorizations to support separation of duties.

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

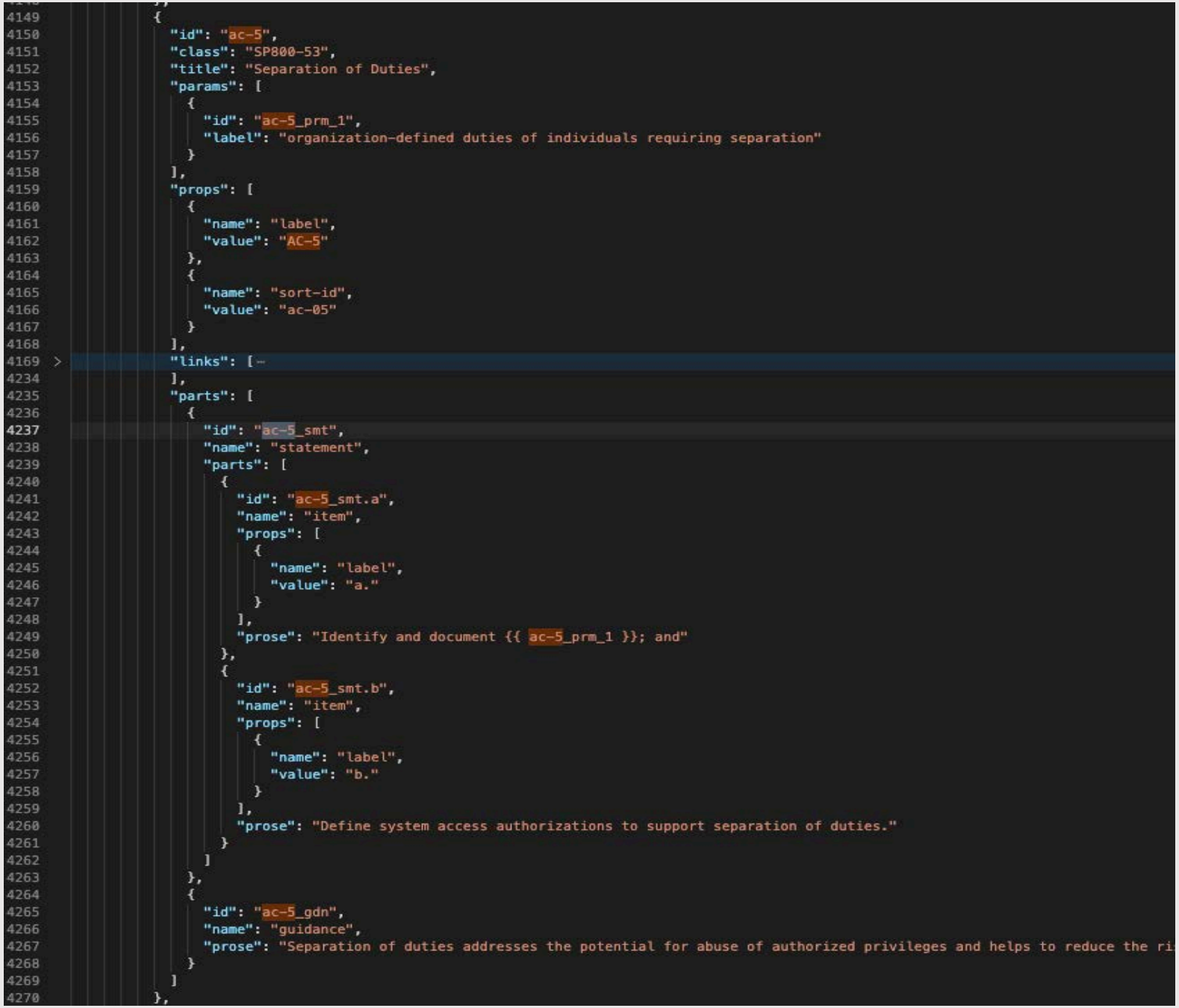
Control Enhancements: None.

References: None.

EXAMPLE 1:
OSCAL CATALOG CONTENT.
THE SP800-53R5 AC-5 CONTROL IN OSCAL XML

```xml
<control class="SP800-53" id="ac-5">
  <title>Separation of Duties</title>
  <param id="ac-5_prm_1">
    <label>organization-defined duties of individuals requiring separation</label>
  </param>
  <prop name="label">AC-5</prop>
  <prop name="sort-id">ac-05</prop>
  <link rel="related" href="#ac-2"/>
  <link rel="related" href="#ac-3"/>
  <link rel="related" href="#ac-6"/>
  <link rel="related" href="#au-9"/>
  <link rel="related" href="#cm-5"/>
  <link rel="related" href="#cm-11"/>
  <link rel="related" href="#cp-9"/>
  <link rel="related" href="#ia-2"/>
  <link rel="related" href="#ia-4"/>
  <link rel="related" href="#ia-5"/>
  <link rel="related" href="#ia-12"/>
  <link rel="related" href="#ma-3"/>
  <link rel="related" href="#ma-5"/>
  <link rel="related" href="#ps-2"/>
  <link rel="related" href="#sa-8"/>
  <link rel="related" href="#sa-17"/>
  <part name="statement" id="ac-5_smt">
    <part name="item" id="ac-5_smt.a">
      <prop name="label">a.</prop>
      <p>Identify and document <insert param-id="ac-5_prm_1"/>; and</p>
    </part>
    <part name="item" id="ac-5_smt.b">
      <prop name="label">b.</prop>
      <p>Define system access authorizations to support separation of duties.</p>
    </part>
  </part>
  <part name="guidance" id="ac-5_gdn">
    <p>Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce t
  </part>
</control>
```

EXAMPLE 1: OSCAL CATALOG CONTENT. THE SP800-53R5 AC-5 CONTROL IN OSCAL JSON



```
{
  "id": "ac-5",
  "class": "SP800-53",
  "title": "Separation of Duties",
  "params": [
    {
      "id": "ac-5_prm_1",
      "label": "organization-defined duties of individuals requiring separation"
    }
  ],
  "props": [
    {
      "name": "label",
      "value": "AC-5"
    },
    {
      "name": "sort-id",
      "value": "ac-05"
    }
  ],
  "links": [...
  ],
  "parts": [
    {
      "id": "ac-5_smt",
      "name": "statement",
      "parts": [
        {
          "id": "ac-5_smt.a",
          "name": "item",
          "props": [
            {
              "name": "label",
              "value": "a."
            }
          ],
          "prose": "Identify and document {{ ac-5_prm_1 }}; and"
        },
        {
          "id": "ac-5_smt.b",
          "name": "item",
          "props": [
            {
              "name": "label",
              "value": "b."
            }
          ],
          "prose": "Define system access authorizations to support separation of duties."
        }
      ]
    },
    {
      "id": "ac-5_gdn",
      "name": "guidance",
      "prose": "Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the ri
    }
  ]
},
```

EXAMPLE 1: OSCAL CATALOG CONTENT. THE SP800-53R5 AC-5 CONTROL IN OSCAL YAML

```yaml
  - id: ac-5
    class: SP800-53
    title: Separation of Duties
    params:
      - id: ac-5_prm_1
        label: organization-defined duties of individuals requiring separation
    props:
      - name: label
        value: AC-5
      - name: sort-id
        value: ac-05
    links: ...
    parts:
      - id: ac-5_smt
        name: statement
        parts:
          - id: ac-5_smt.a
            name: item
            props:
              - name: label
                value: a.
            prose: Identify and document {{ ac-5_prm_1 }}; and
          - id: ac-5_smt.b
            name: item
            props:
              - name: label
                value: b.
            prose: Define system access authorizations to support separation of duties.
      - id: ac-5_gdn
        name: guidance
        prose: Separation of duties addresses the potential for abuse of authorized privileges
  -
```

EXAMPLE 2: OSCAL CATALOG CONTENT
THE 27002 CONTROL 6.1.2 (PROSE)

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls. Small organizations may find segregation of duties difficult to achieve, but the principle should be

applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

Other information

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

EXAMPLE 2:
OSCAL CATALOG CONTENT.
THE 27002 6.1.2 CONTROL IN OSCAL XML

```
<control id="s6.1.2">
   <title>Segregation of duties</title>
   <prop name="label">6.1.2</prop>
   <part id="s6.1.2_stm" name="statement">
      <p>Conflicting duties and areas of responsibility should be segregat
   </part>
   <part id="s6.1.2_gdn" name="guidance">
      <part id="s6.1.2_gdn.1" name="item">
         <p>Care should be taken that no single person can access, modify
      </part>
      <part id="s6.1.2_gdn.2" name="item">
         <p>Small organizations may find segregation of duties difficult t
      </part>
   </part>
   <part id="s6.1.2_inf" name="information">
      <p>Segregation of duties is a method for reducing the risk of accide
   </part>
</control>
```

EXAMPLE 2: OSCAL CATALOG CONTENT. THE 27002 6.1.2 CONTROL IN OSCAL JSON

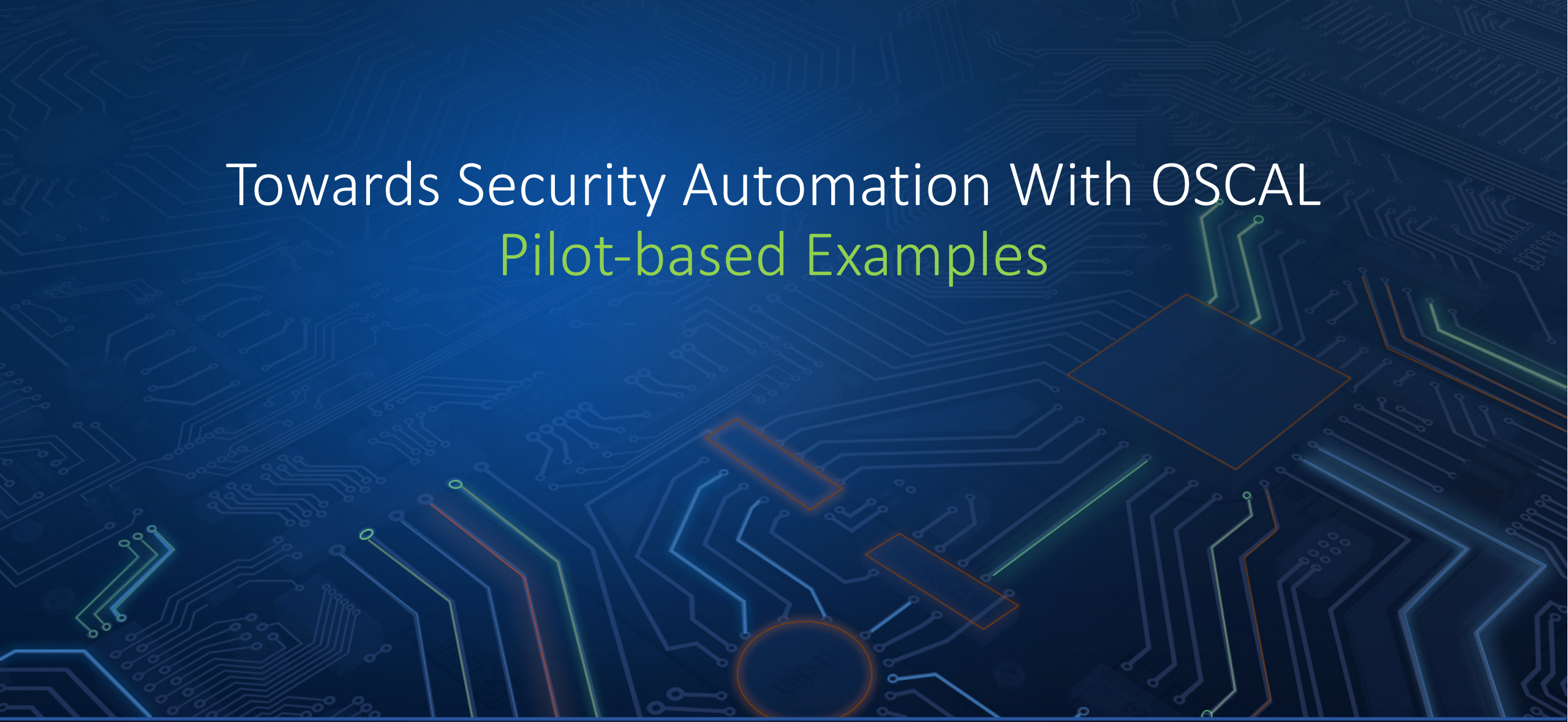

```
{
  "id": "s6.1.2",
  "title": "Segregation of duties",
  "props": [
    {
      "name": "label",
      "value": "6.1.2"
    }
  ],
  "parts": [
    {
      "id": "s6.1.2_stm",
      "name": "statement",
      "prose": "Conflicting duties and areas of responsibility should be segregated to reduce opportunities
    },
    {
      "id": "s6.1.2_gdn",
      "name": "guidance",
      "parts": [
        {
          "id": "s6.1.2_gdn.1",
          "name": "item",
          "prose": "Care should be taken that no single person can access, modify or use assets without autho
        },
        {
          "id": "s6.1.2_gdn.2",
          "name": "item",
          "prose": "Small organizations may find segregation of duties difficult to achieve, but the princip
        }
      ]
    },
    {
      "id": "s6.1.2_inf",
      "name": "information",
      "prose": "Segregation of duties is a method for reducing the risk of accidental or deliberate misuse o
    }
  ]
}
```

EXAMPLE 2:
OSCAL CATALOG CONTENT.
THE 27002 6.1.2 CONTROL IN OSCAL YAML

```yaml
-
  id:    s1.1.2
  title: Segregation of duties
  props:
    -
      name:  label
      value: 1.1.2
  parts:
    -
      id:    s1.1.2_stm
      name:  statement
      prose: Conflicting duties and areas of responsibility should be segregated to reduce opportunit
    -
      id:    s1.1.2_gdn
      name:  guidance
      parts:
        -
          id:    s1.1.2_gdn.1
          name:  item
          prose: Care should be taken that no single person can access, modify or use assets without
        -
          id:    s1.1.2_gdn.2
          name:  item
          prose: Small organizations may find segregation of duties difficult to achieve, but the pri
    -
      id:    s1.1.2_inf
      name:  information
      prose: Segregation of duties is a method for reducing the risk of accidental or deliberate misu
```

Towards Security Automation With OSCAL

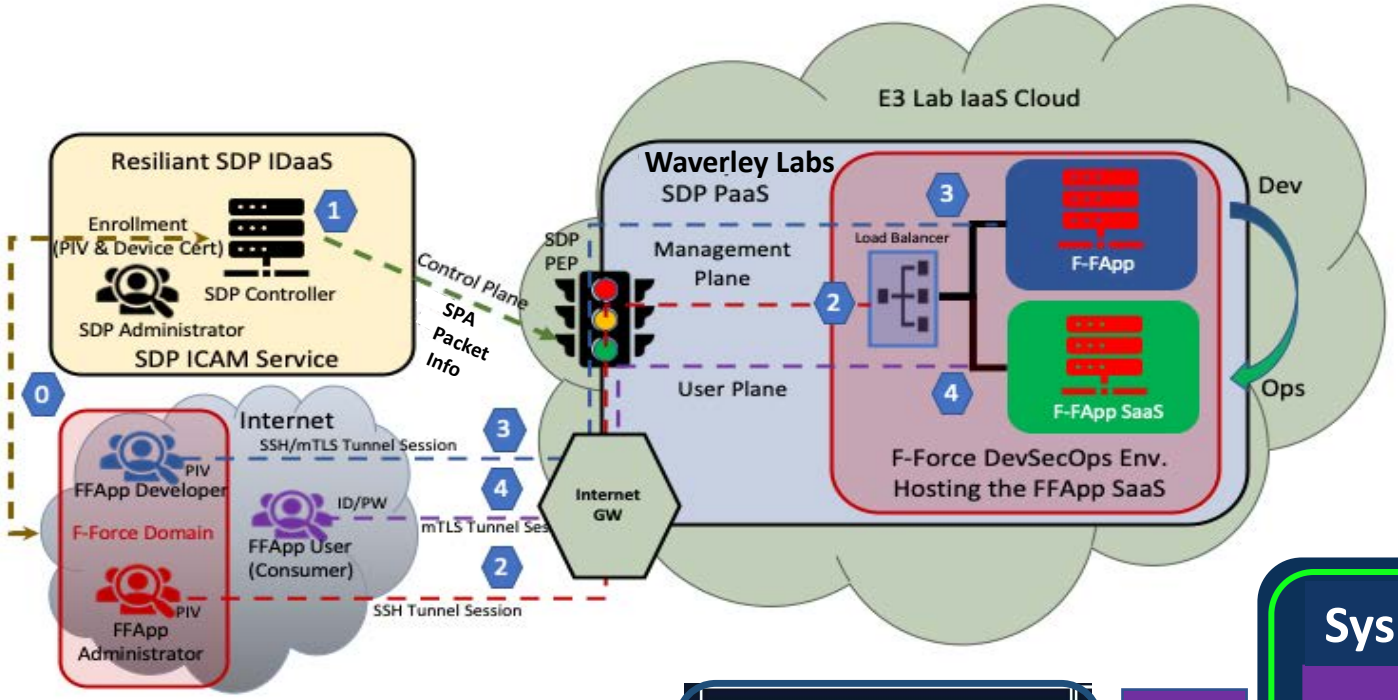
Pilot-based Examples

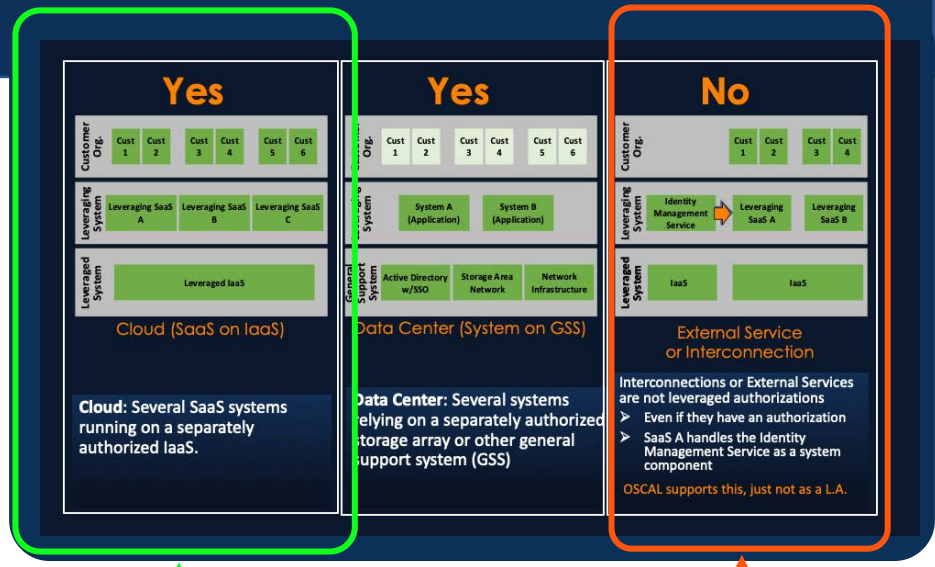


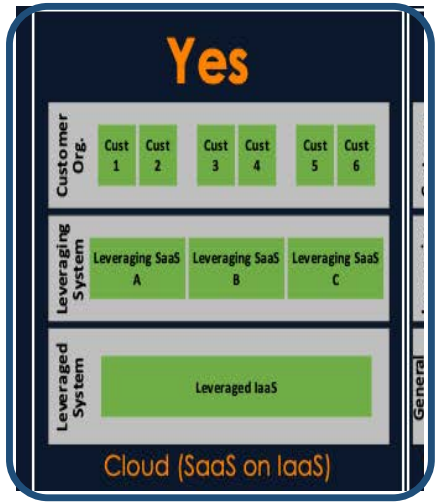
National Institute of Standards and Technology
U.S. Department of Commerce

Example 1: ZTA & DevSecOps Pilot

High Level Architecture







SaaS

PaaS

IaaS

Sys Sec Responsibility Stack

F-Force App Consumer

F-Force App [System Owner]

Waverley SDP PaaS [CSP2]

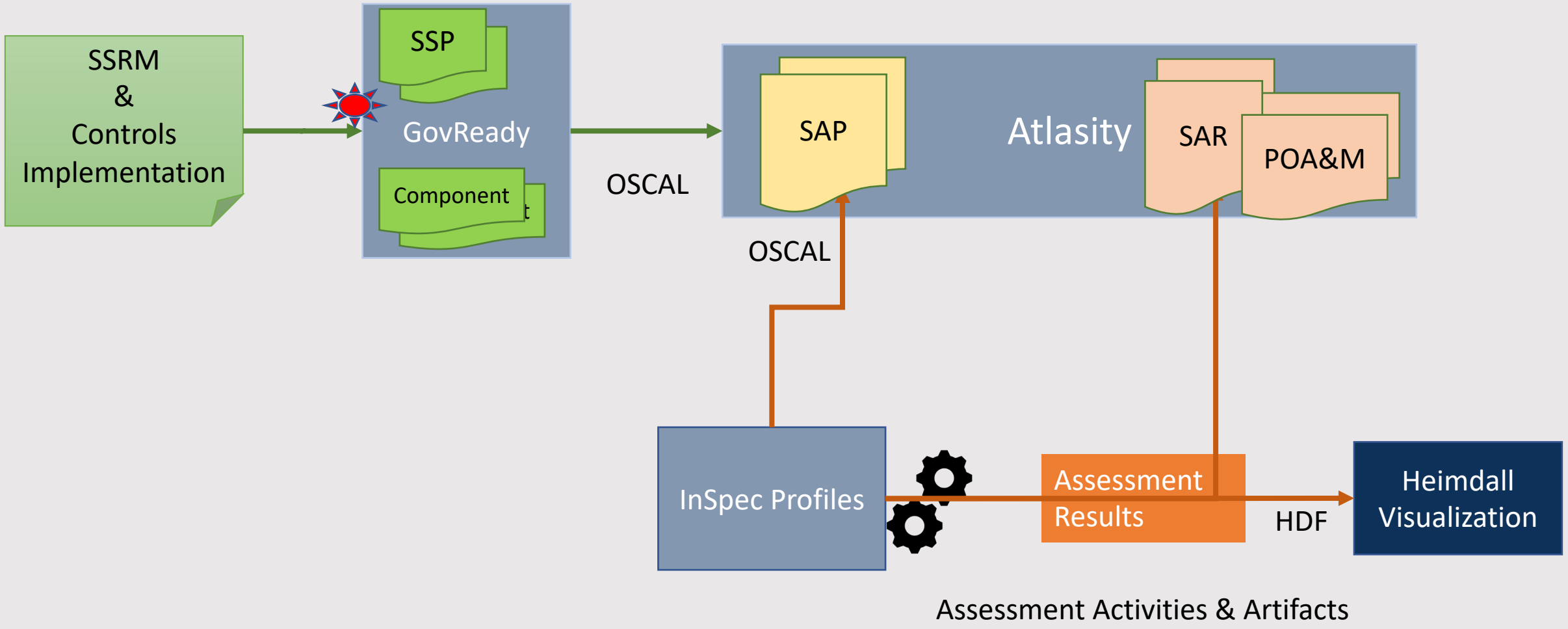
2 Twelve E3 Lab IaaS [CSP1]

Interconnected System

Resiliant SDP IDaaS

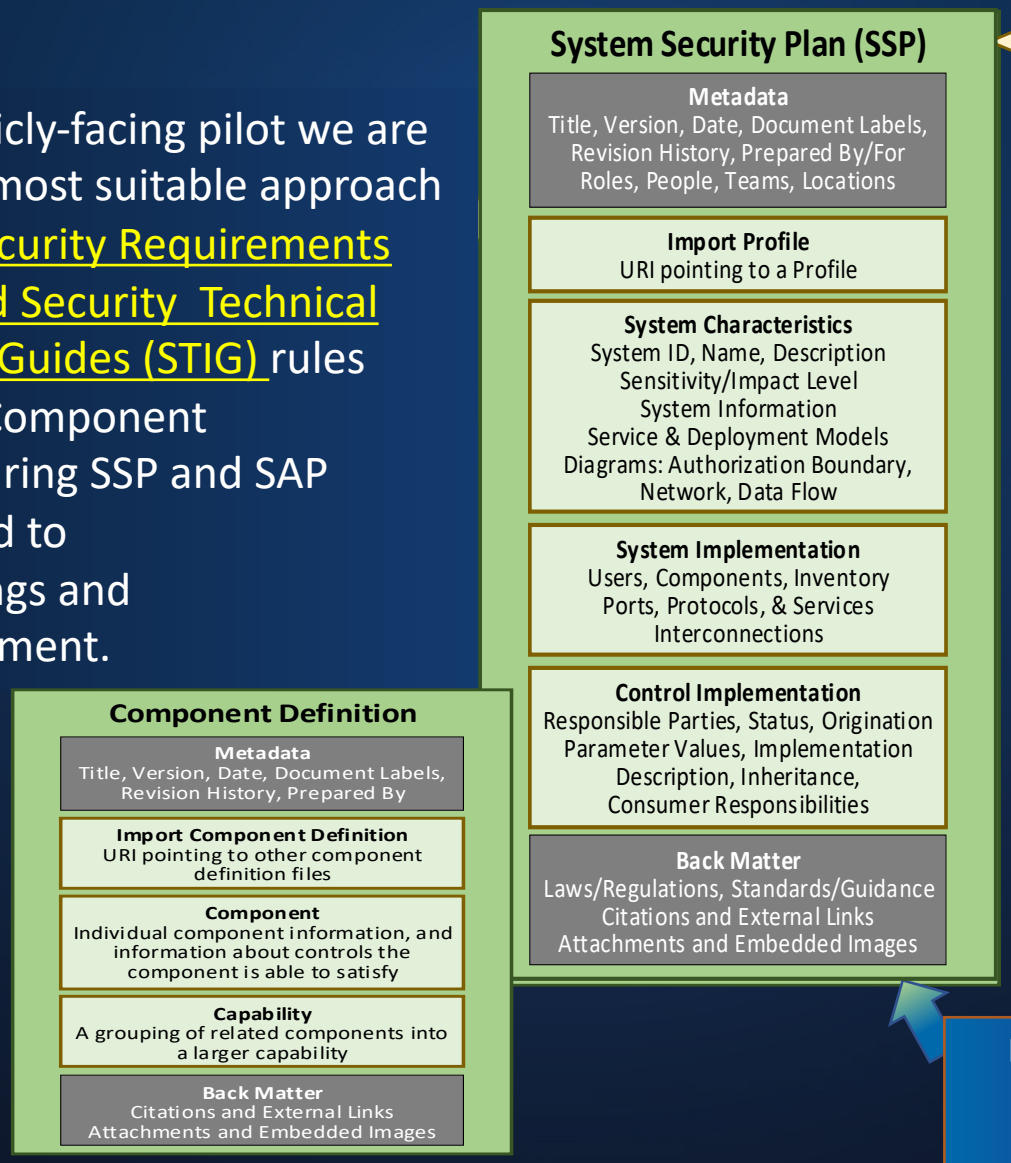
Example 3: ZTA & DevSecOps Pilot
The OSCAL-enabled Toolchain

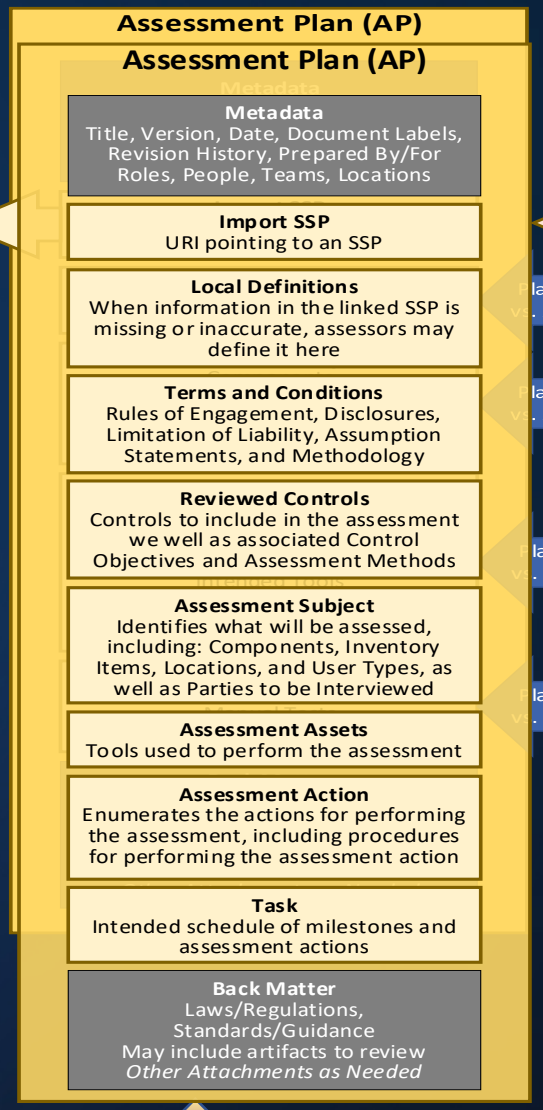
A&A Documentation Pipeline

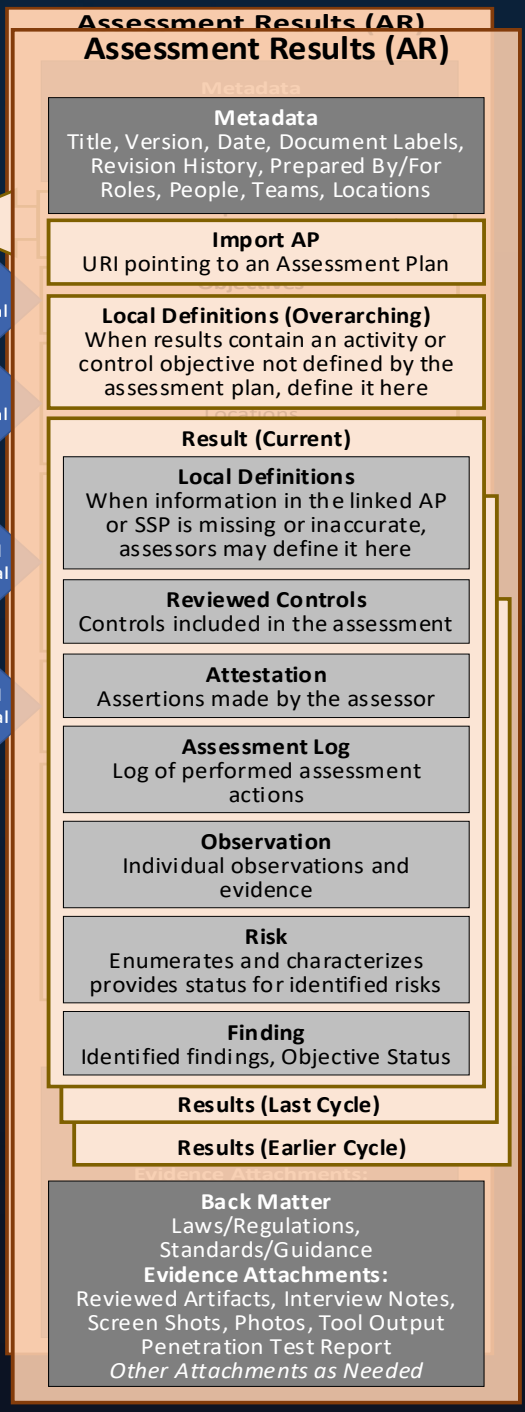


Example 4:
OSCAL Component & DoD's STIGs

As part of a publicly-facing pilot we are researching the most suitable approach for leveraging Security Requirements Guides (SRG) and Security Technical Implementation Guides (STIG) rules through OSCAL Component model for use during SSP and SAP development and to report SAR findings and POA&M development.







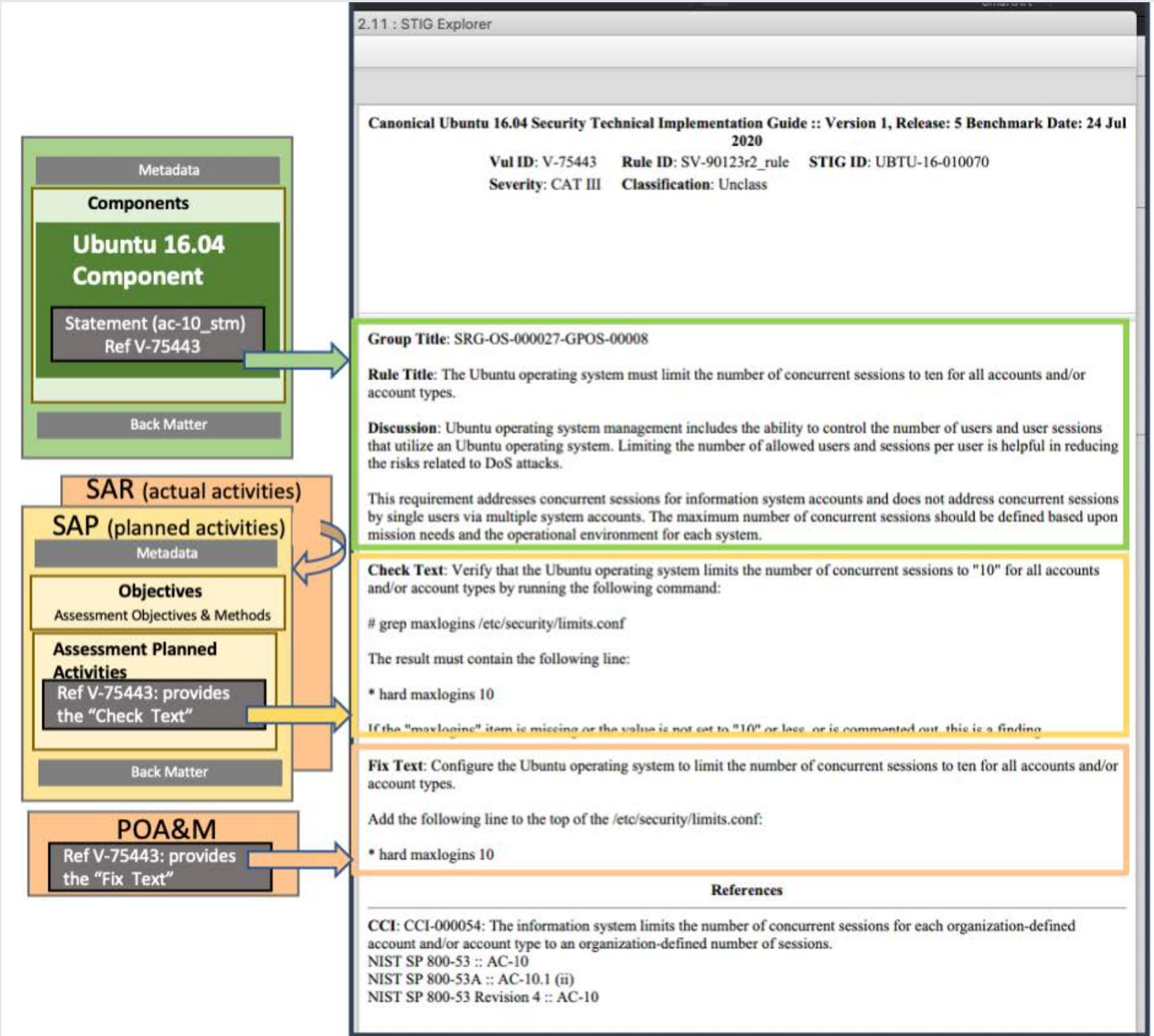
DoD Security Requirements Guides (SRGs) and DoD Security Technical Implementation Guides (STIGs)

Example 4:

STIG Data [V-# Rule]

vs

OSCAL Data



OSCAL CONTENT (M3): CANONICAL UBUNTU 16.04.04 LTS COMPONENT SAMPLE


```
{ "$schema": "./schema/oscal_component_schema.json",
  "component-definition": {
    "metadata": {
      "title": "Canonical Ubuntu 16.04 LTS",
      "last-modified": "2020-08-12T19:24:24.389Z",
      "version": "Version 1",
      "oscal-version": "1.0.0-milestone3",
      "document-ids": [ {
        "identifier": "some-identifier-locally defined or doi",
        "type": "guidance" } ],
      "parties": [  {
        "uuid": "ee47836c-877c-4007-bbf3-c9d9bd805a9a",
        "party-name": "MI  Co",
        "type": "organization" } ] },
    "components": {
      "b036a6ac-6cff-4066-92bc-74ddfd9ad6fa": {
          "name": "Ubuntu 16.04 Implementation",
        "component-type": "software",
        "title": "Ubuntu 16.04 Implementation",
        "description": "Ubuntu operating system implementation of the CCI-based profile of SP 800-53 rev controls per [pointer to Canonical Ubuntu 16.04 LTS STIG].",
        "responsible-parties": {  "supplier": { "party-uuids": [ "ee47836c-877c-4007-bbf3-c9d9bd805a9a"  ] } },
        "control-implementations": [  {
          "uuid": "cfcdd674-8595-4f98-a9d1-3ac70825c49f",
          "source": "../../../some/path/to/SP-800-53_rev4_profile.json",
          "description": "Ubuntu 16.04 recommended implementation of the AC-10 control for the CCI-based profile of SP 800-53 rev4 controls.",
          "implemented-requirements": [  {
            "uuid": "d1016df0-9b5c-4839-86cd-f9c1d113077b",
            "control-id": "ac-10",
            "set-parameters":  {
              "ac-10_prm_1" : { "value" : "all accounts and all types of accounts" },
              "ac-10_prm_2" : { "value" : "10" }  },
            "description": "Ubuntu operating system is configured to limit the number of concurrent sessions for the accounts specified by the account-type parameter to the max-sessions parameter.",
            "statements": {
              "ac-10_stm" : {
                "uuid" : "fb4d039a-dc4f-46f5-9c1f-f6343eaf69bc",
                "description": "This provides the configuration for limiting concurrent sessions.",
                "links": [ {
                  "href": "#090ab379-2089-4830-b9fd-26d0729e22e9",
                  "text": "V-75443",
                  "rel": "assessment-method"  } ] }
              } } ] } ] } },
  "back-matter": {
    "resources": [  {
      "uuid" : "090ab379-2089-4830-b9fd-26d0729e22e9",
      "title" : "V-75443",
      "desc" : "STIG document Vul ID",
      "rlinks" : [ {
        "media-type": "application/inspec+ruby",
        "href" : "https://github.com/mitre/canonical-ubuntu-16.04-lts-stig-baseline/blob/master/controls/V-75443.rb"
    } ] } ] } } }
```


XCCDF FILE IS PREFERRED

Example 4:

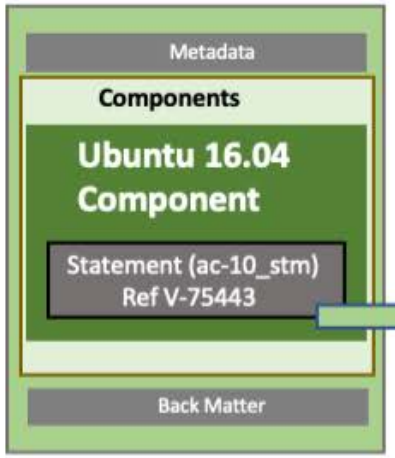
STIG Data [V-# Rule]

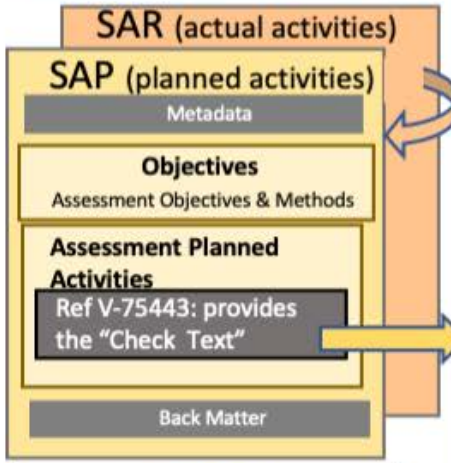
vs

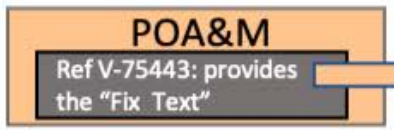
OSCAL Data

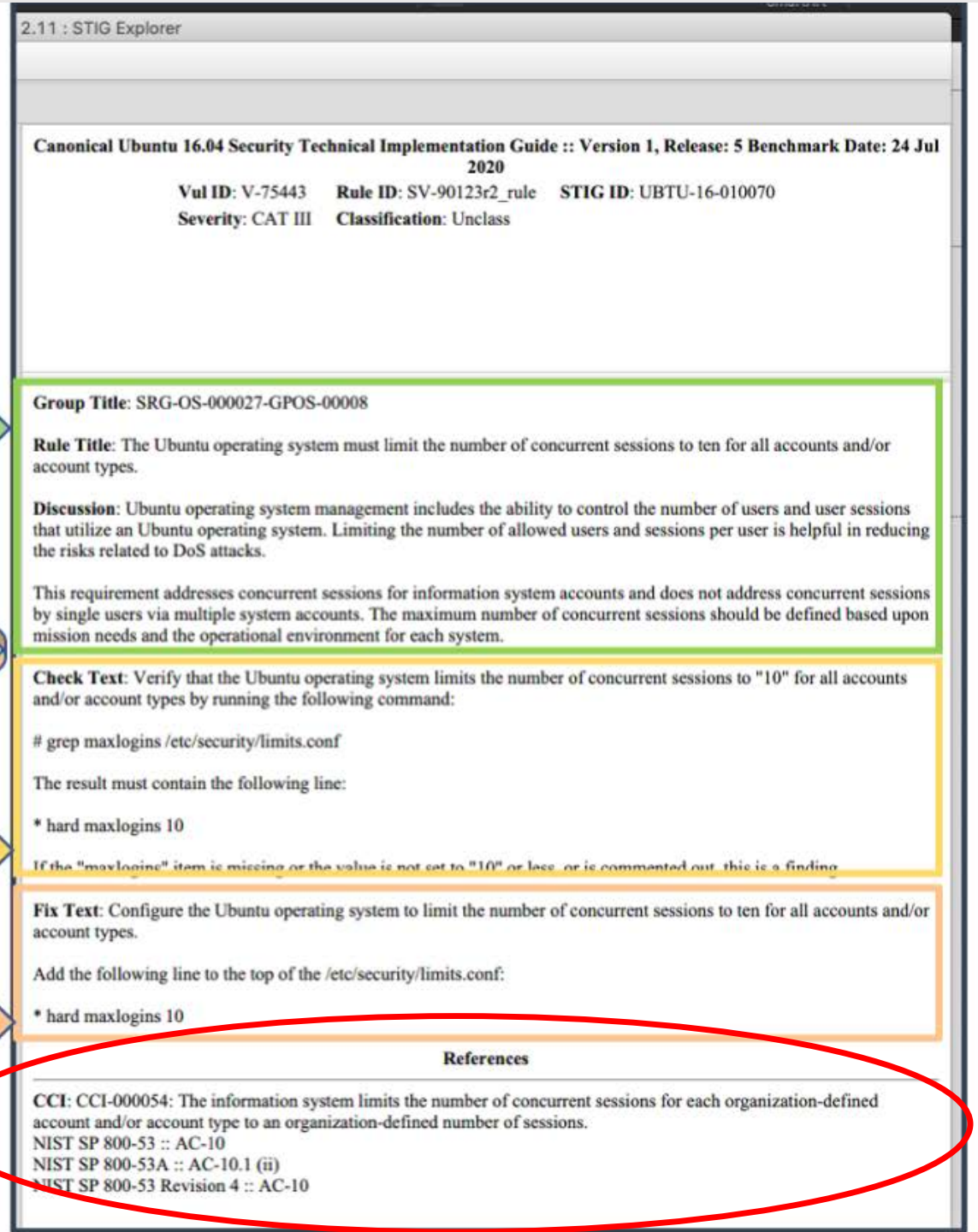
Control Correlation Identifiers

A CALL FOR COLLABORATION:
PLEASE JOIN US ON GITTER TO BRAINSTORM THE BEST SOLUTION
https://gitter.im/usnistgov-OSCAL/CCIs









Questions?