

OSCAL Content

February 2, 2021

Open Security Controls nt Language

Contribute **Contact Us Futorials** Documentation Downloads Tools

OSCAL

atomated ontrol-Based ssessment

upporting Control-Based Risk Management with Standardized Formats

Learn More

AC-19 V C-19(5) V AC-20(1) AC-20 √ AC-21 DM AC-22 J AT-1 √ AT-2(2) √ AT-2 J AT-4

iding control-related nation in machine-¹e formats.

NIST, in collaboration with industry, is developing the Open Security Controls Assessment La of formats expressed in XML, JSON, and YAML. These formats provide machine-readable reprecontrol baselines, system security plans, and assessment plans and results.



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
•	ovamplas	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
	fodramp.gov		SP 800-53 NIST Low Baseline	Rev 5	NIST SP 800-53 Rev5B
	nist.gov/SP800-53 oscal @ d26e3b3		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
	<u>src</u>	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

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:
 <u>catalog</u>: This directory contains sample content for the OSCAL <u>catalog</u> model.
 - <u>component-definition</u>: This directory contains sample content for the OSCAL <u>component definition</u> model.
 <u>ssp</u>: This directory contains sample content for the OSCAL <u>system security plan</u> (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

<u>Control</u>:

- a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and
- b. Define system access authorizations to support separation of duties.

<u>Discussion</u>: 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 <u>AC-2</u>, access control mechanisms in <u>AC-3</u>, and identity management activities in <u>IA-2</u>, <u>IA-4</u>, and <u>IA-12</u>.

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

Control Enhancements: None.

References: None.

EXAMPLE 1: OSCAL CATALOG CONTENT. THE SP800-53R5 AC-5 CONTROL IN OSCAL 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> k rel="related" href="#ac-2"/> k rel="related" href="#ac-3"/> link rel="related" href="#ac-6"/> k rel="related" href="#au-9"/> k rel="related" href="#cm-5"/> k rel="related" href="#cm-11"/> k rel="related" href="#cp-9"/> k rel="related" href="#ia-2"/> k rel="related" href="#ia-4"/> k rel="related" href="#ia-5"/> k rel="related" href="#ia-12"/> k rel="related" href="#ma-3"/> k rel="related" href="#ma-5"/> k rel="related" href="#ps-2"/> k rel="related" href="#sa-8"/> k 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> Identify and document <insert param-id="ac-5_prm_1"/>; and </part> <part name="item" id="ac-5_smt.b"> <prop name="label">b.</prop> Define system access authorizations to support separation of duties. </part> </part> <part name="guidance" id="ac-5_gdn"> Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce </part> </control>

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



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

2999	
3000	id: ac-5
3001	class: SP800-53
3002	title: Separation of Duties
3003	params:
3004	
3005	id: ac-5_prm_1
3006	label: organization-defined duties of individuals requiring separation
3007	props:
3008	
3009	name: label
3010	value: AC-5
3011	
3012	name: sort-id
3013	value: ac-05
3014 >	links:
3063	parts:
3064	
3065	id: ac-5_smt
3066	name: statement
3067	parts:
3068	
3069	id: ac-5_smt.a
3070	name: item
3071	props
3072	
3073	name: label
3074	value: a.
3075	<pre>prose: Identify and document {{ ac-5_prm_1 }}; and</pre>
3076	
3077	id: ac-5_smt.b
3078	name: item
3079	props:
3080	
3081	name: label
3082	value: b.
3083	prose: Define system access authorizations to support separation of duties.
3084	
3085	id: ac-5_gdn
3086	name: guidance
3087	prose: Separation of duties addresses the potential for abuse of authorized privileges
3088	

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

6.1.2 Segregation of duties

<u>Control</u>

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">
      <Conflicting duties and areas of responsibility should be segregat</p>
  </part>
   <part id="s6.1.2_gdn" name="guidance">
     <part id="s6.1.2_gdn.1" name="item">
         Care should be taken that no single person can access, modify
     </part>
     <part id="s6.1.2_gdn.2" name="item">
         Small organizations may find segregation of duties difficult in
     </part>
   </part>
   <part id="s6.1.2_inf" name="information">
     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 authout
      },
        "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

s1.1.2 id: title: S@gregation of duties props: label name: value: 1.1.2 6 parts: s1.1.2 stm id: soatement name: prose: Conflicting duties and areas of responsibility should be segregated to reduce opportunit s1.1.2_gdn id: glidance name: parts: s1.1.2_gdn.1 id: i Gem name: prose: Care should be taken that no single person can access, modify or use assets without s1.1.2_gdn.2 id: i Gem name: prose: Small organizations may find segregation of duties difficult to achieve, but the pri s1.1.2 inf id: information name: prose: Segregation of duties is a method for reducing the risk of accidental or deliberate misu

Towards Security Automation With OSCAL Pilot-based Examples





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

A&A Documentation Pipeline



Assessment Activities & Artifacts

Example 4: OSCAL Component & DoD's STIGs

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

Component Definition Metadata Title. Version. Date. Document Labels. **Revision History, Prepared By** Import Component Definition URI pointing to other component definition files Component Individual component information, and information about controls the component is able to satisfy Capability A grouping of related components into a larger capability **Back Matter Citations and External Links** Attachments and Embedded Images

System Security Plan (SSP)

Metadata Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import Profile URI pointing to a Profile

System Characteristics System ID, Name, Description Sensitivity/Impact Level System Information Service & Deployment Models Diagrams: Authorization Boundary, Network, Data Flow

System Implementation Users, Components, Inventory Ports, Protocols, & Services Interconnections

Control Implementation Responsible Parties, Status, Origination Parameter Values, Implementation Description, Inheritance, Consumer Responsibilities

Back Matter Laws/Regulations, Standards/Guidance Citations and External Links Attachments and Embedded Images

Assessment Plan (AP) Assessment Plan (AP)

Metadata Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import SSP URI pointing to an SSP

Local Definitions When information in the linked SSP is missing or inaccurate, assessors may define it here

anned

Actual

anned

Actua

lanned

. Actua

lanned

Actua

Terms and Conditions Rules of Engagement, Disclosures, Limitation of Liability, Assumption Statements, and Methodology

Reviewed Controls Controls to include in the assessment we well as associated Control Objectives and Assessment Methods

Assessment Subject Identifies what will be assessed, including: Components, Inventory Items, Locations, and User Types, as well as Parties to be Interviewed

Assessment Assets Tools used to perform the assessment

Assessment Action Enumerates the actions for performing the assessment, including procedures for performing the assessment action

Task Intended schedule of milestones and assessment actions

Back Matter Laws/Regulations, Standards/Guidance May include artifacts to review Other Attachments as Needed

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

Assessment Results (AR) Assessment Results (AR)

Metadata Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import AP URI pointing to an Assessment Plan

Local Definitions (Overarching) When results contain an activity or control objective not defined by the assessment plan, define it here

Result (Current)

Local Definitions When information in the linked AP or SSP is missing or inaccurate, assessors may define it here

Reviewed Controls Controls included in the assessment

Attestation Assertions made by the assessor

Assessment Log Log of performed assessment actions

Observation Individual observations and evidence

Risk Enumerates and characterizes provides status for identified risks

Finding Identified findings, Objective Status

Results (Last Cycle)

Results (Earlier Cycle)

Back Matter

Laws/Regulations, Standards/Guidance Evidence Attachments: Reviewed Artifacts, Interview Notes, Screen Shots, Photos, Tool Output Penetration Test Report Other Attachments as Needed

Example 4: STIG Data [V-# Rule] vs OSCAL Data

	Canonical Ubuntu 16.04 Security Technical Implementation Guide :: Version 1, Release: 5 Benchmark Date: 24 Jul 2020		
Metadata	Vul ID: V-75443 Rule ID: SV-90123r2_rule STIG ID: UBTU-16-010070		
ivietadata	Severity: CAT III Classification: Unclass		
Components			
Ubuntu 16.04 Component			
Statement (ac-10_stm) Ref V-75443	Group Title: SRG-OS-000027-GPOS-00008		
	Rule Title: The Ubuntu operating system must limit the number of concurrent sessions to ten for all accounts and/or account types.		
Back Matter	Discussion: Ubuntu operating system management includes the ability to control the number of users and user sessions that utilize an Ubuntu operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.		
SAR (actual activities) SAP (planned activities)	This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.		
Objectives	Check Text: Verify that the Ubuntu operating system limits the number of concurrent sessions to "10" for all accounts and/or account types by running the following command:		
Assessment Objectives & Methods	# grep maxlogins /etc/security/limits.conf		
Assessment Planned Activities	The result must contain the following line:		
Ref V-75443: provides	* hard maxlogins 10		
the "Check Text"	If the "maxlagine" item is missing or the value is not set to "10" or less or is commented out, this is a finding		
Back Matter	Fix Text: Configure the Ubuntu operating system to limit the number of concurrent sessions to ten for all accounts and/or account types.		
POA8M	Add the following line to the top of the /etc/security/limits.conf:		
Ref V-75443: provides	* hard maxlogins 10		
the "Fix Text"	References		
	CCI: CCI-000054: The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions. NIST SP 800-53 :: AC-10 NIST SP 800-53A :: AC-10.1 (ii) NIST SP 800-53 Revision 4 :: AC-10		

```
"$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": [ {
OSCAL CONTENT (M3):
                                                                 "uuid": "cfcdd674-8595-4f98-a9d1-3ac70825c49f".
                                                                 "source": "../../../some/path/to/SP-800-53 rev4 profile.json",
CANONICAL UBUNTU
                                                                 "description": "Ubuntu 16.04 recommended implementation of the AC-10 control for the CCI-based profile of SP 800-53 rev4 controls.",
                                                                 "implemented-requirements": [ {
16.04.04 LTS
                                                                      "uuid": "d1016df0-9b5c-4839-86cd-f9c1d113077b",
                                                                     "control-id": "ac-10",
COMPONENT SAMPLE
                                                                     "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":
                                                                                                                                                             XCCDF FILE IS PREFERRED
                                                         "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"
                                                        } ] } ] } }
```

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

	_
Metadata Components Ubuntu 16.04	Canonical Ubuntu 16.04 Security Technical Implementation Guide :: Version 1, Release: 5 Benchmark Date: 24 Jul 2020 Vul ID: V-75443 Rule ID: SV-90123r2_rule STIG ID: UBTU-16-010070 Severity: CAT III Classification: Unclass
Statement (ac-10_stm) Ref V-75443	Group Title: SRG-OS-000027-GPOS-00008 Rule Title: The Ubuntu operating system must limit the number of concurrent sessions to ten for all accounts and/or account types.
Back Matter SAR (actual activities)	Discussion: Ubuntu operating system management includes the ability to control the number of users and user sessions that utilize an Ubuntu operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks. This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon
Metadata Objectives Assessment Objectives & Methods	mission needs and the operational environment for each system. Check Text: Verify that the Ubuntu operating system limits the number of concurrent sessions to "10" for all accounts and/or account types by running the following command: # grep maxlogins /etc/security/limits.conf
Assessment Planned Activities Ref V-75443: provides the "Check Text"	The result must contain the following line: * hard maxlogins 10 If the "maxlogine" item is missing or the value is not set to "10" or less, or is commented out, this is a finding
Back Matter	Fix Text: Configure the Ubuntu operating system to limit the number of concurrent sessions to ten for all accounts and/or account types. Add the following line to the top of the /etc/security/limits.conf:
Ref V-75443: provides the "Fix Text"	hard maxlogins 10 References
	CCI: CCI-000054: The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions. NIST SP 800-53 :: AC-10 NIST SP 800-53A :: AC-10.1 (ii) NIST SP 800-53 Revision 4 :: AC-10

2.11 : STIG Explorer

Questions?