Security Automation with Open Security Controls Assessment Language (OSCAL)

May 26, 2021

Dr. Michaela Iorga,
OSCAL Strategic Outreach Director

Dave Waltermire,
OSCAL Technical Director
Why we care?

Today’s challenges:

- Information technology is complex
- Security vulnerabilities are everywhere
- Regulatory frameworks are burdensome
- Risk management is hard
- Documentation becomes outdated fast
OSCAL sets the foundation for automation and interoperability.

OSCAL is like a Rosetta Stone that enables tools and organizations to exchange information via automation.

What was needed?

- Catalog Authors
- Baseline Authors
- Security Professionals
- Assessors & Auditors
- Tools to Document Assessment
- Tools to Assess IT Assets
- Tools to Manage IT Assets
- Tools to Report Status

OSCAL sets the foundation for automation and interoperability.
OSCAL is the result of NIST and FedRAMP collaboration

- **OSCAL provides** a common/single machine-readable *language*, expressed in XML, JSON and YAML for:
  - multiple compliance and risk management frameworks (e.g. SP 800-53, ISO/IEC 27001&2, COBIT 5)
  - software and service providers to express implementation guidance against security controls (Component definition)
  - sharing how security controls are implemented (System Security Plans [SSPs])
  - sharing security assessment plans (System Assessment Plans [SAPs])
  - sharing security assessment results/reports (System Assessment Results [SARs])

- **OSCAL enables automated traceability** from selection of security controls through implementation and assessment
OSCAL 1.0.0 Architecture

Layers & Models

- **Assessment Results Layer**
  - Plan of Action and Milestones (POA&M) Model
  - Assessment Results Model
  - Possible Other Assessment Results Model (Future)

- **Assessment Layer**
  - Assessment Plan Model
  - Assessment Activities Model(s) (Future)

- **Implementation Layer**
  - System Security Plan Model
  - Component Definition Model

- **Profile Layer**
  - Profile Model

- **Catalog Layer**
  - Catalog Model

DHS OCISO FY21 Spring Symposium
OSCAL SSP:

- Imports a Profile identifying the controls
- Each control response is broken down to the individual components involved.
- Enables a more robust response to controls
- Example: The access control implementation that satisfies AC-2, part a is described separately for:
  - This System
  - The Access Control Procedure
  - A shared Application
Assessment Plan (SAP) & Assessment Results (AR)

- OVERLAPPING SYNTAX
- SIMILAR BUT DISTINCT PURPOSE
- UNIQUE to AR: Results and Evidence

Continuous Assessment Approach

- Assessment Plan: What should be tested/inspected, how, and with which frequency
- Assessment Results: Time-slice of results

Planed activities ↔ Actual activities
Assessment Results & POA&Ms Overlapping Syntax

### Assessment Results

<table>
<thead>
<tr>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import AP</td>
</tr>
<tr>
<td>Objectives</td>
</tr>
<tr>
<td>Results (Current)</td>
</tr>
<tr>
<td>Local Definitions</td>
</tr>
<tr>
<td>Reviewed Controls</td>
</tr>
<tr>
<td>Assessment Subject</td>
</tr>
<tr>
<td>Assessment Assets</td>
</tr>
<tr>
<td>Attestations / Assessment Log</td>
</tr>
</tbody>
</table>

#### Finding

**Objective Status**
- Assessment Objective ID

**Observations**
- Risk Information
  - Title, Source, CVE#, Calculations, Severity, Recommendations

**Status**
- "open"

**Vendor Dependencies**
- Status and Evidence

**Deviations**
- Justification
- False Positive (FP)
- Operational Requirement (OR)
- Risk Adjustment (RA)

**SSP Implementation Statement Differential**

**Finding (From Automated Tools / Scanners)**

**Finding (From Penetration Testing)**

### Plan of Action and Milestones (POA&M)

<table>
<thead>
<tr>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import SSP</td>
</tr>
<tr>
<td>System Identifier</td>
</tr>
<tr>
<td>Local Definitions, Observations, Risks</td>
</tr>
</tbody>
</table>

#### POA&M Items

- POA&M Item
  - Unique ID, Impacted Control

- Observations
  - Risk Information
    - Title, Source, CVE#, Severity

- Remediation Activities
  - Plan, Schedule, Resolution Date, Remediation Status

- Vendor Dependencies
  - Evidence and Check-Ins

**Deviations**
- Status (Investigating, Pending, Approved)
- False Positive (FP)
- Operational Requirement (OR)
- Risk Adjustment (RA)

**CVSS Metrics**

Risks with status="open" at the end of testing are transferred to the POA&M using the same OSCAL syntax. Corresponding observations must also be transferred.
OSCAL: the Open Security Controls Assessment Language

Automated Control-Based Assessment
Supporting Control-Based Risk Management with Standardized Formats

Providing control-related information in machine-readable formats.

NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.
OSCAL MODELS vs. OSCAL CONTENT

**OSCAL MODELS**
- OSCAL Catalog Model
- OSCAL Profile Model
- OSCAL Component Model
- OSCAL SSP Model
- OSCAL Assessment Plan Model
- OSCAL Assessment Results Model
- OSCAL Plan of Action and Milestones Model

**OSCAL CONTENT**
- Catalog in OSCAL
- Profile in OSCAL
- Component in OSCAL
- Assessment Plan in OSCAL
- Assessment Results in OSCAL
- SSP in OSCAL
- Plan of Action and Milestones in OSCAL
OSCAL Content vs OSCAL Tools

OSCAL GRC TOOLCHAIN

CATALOG & PROFILE EDITORS

COMPONENT & SSP EDITORS

ASSESSMENT PLANNING

ASSESSMENT ACTIVITIES & RESULTS

CATALOG & PROFILE

EDITORS

COMPONENT & SSP
EDITORS

ASSESSMENT

PLANNING

ASSESSMENT

ACTIVITIES & RESULTS
## OSCAL CONTENT (XML, JSON, YAML) Catalogs and Profiles

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

<table>
<thead>
<tr>
<th>Maintainer</th>
<th>OSCAL Information</th>
<th>Source Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>SP 800-53 Catalog</td>
<td>Rev 4 NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Low Baseline</td>
<td>Rev 4 NIST SP 800-53 Rev4</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Moderate Baseline</td>
<td>Rev 4 NIST SP 800-53 Rev4</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST High Baseline</td>
<td>Rev 4 NIST SP 800-53 Rev4</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Resolved Low Baseline</td>
<td>Rev 4 NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Resolved Moderate Baseline</td>
<td>Rev 4 NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Resolved High Baseline</td>
<td>Rev 4 NIST SP 800-53 Rev4 + NIST SP 800-53A Rev4</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 Catalog</td>
<td>Rev 5 NIST SP 800-53 Rev5</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Low Baseline</td>
<td>Rev 5 NIST SP 800-53 Rev5B</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Moderate Baseline</td>
<td>Rev 5 NIST SP 800-53 Rev5B</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST High Baseline</td>
<td>Rev 5 NIST SP 800-53 Rev5B</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 NIST Privacy Baseline</td>
<td>Rev 5 NIST SP 800-53 Rev5B</td>
</tr>
</tbody>
</table>
OSCAL (XML, JSON, YAML) Examples

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

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

- The content of the ‘examples’ directory is 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.

- Examples do not represent real data
FedRAMP OSCAL (XML, JSON and YAML) Profiles

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

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

<table>
<thead>
<tr>
<th>Maintainer</th>
<th>OSCAL Information</th>
<th>Source Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>FedRAMP</td>
<td>SP 800-53 FedRAMP Low Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 FedRAMP Moderate Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 FedRAMP High Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 FedRAMP Tailored Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 FedRAMP Resolved Low Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 FedRAMP Resolved Moderate Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 FedRAMP Resolved High Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
<tr>
<td></td>
<td>SP 800-53 FedRAMP Resolved Tailored Baseline</td>
<td>FedRAMP Security Controls Baselines</td>
</tr>
</tbody>
</table>
Authorization to Use & Common Control Authorization
### Cloud (SaaS on IaaS)

Cloud: Several SaaS systems running on a separately authorized IaaS.

### Yes

- **Customer Org.:**
  - Cust 1
  - Cust 2
  - Cust 3
  - Cust 4
  - Cust 5
  - Cust 6

- **Leveraging System:**
  - Leveraging SaaS A
  - Leveraging SaaS B
  - Leveraging SaaS C

- **Authorization to Use:** Leveraged IaaS

### Data Center (System on GSS)

- **Customer Org.:**
  - Cust 1
  - Cust 2
  - Cust 3
  - Cust 4
  - Cust 5
  - Cust 6

- **Leveraging System:**
  - System A (Application)
  - System B (Application)

- **General Support System:**
  - Active Directory w/SSO
  - Storage Area Network
  - Network Infrastructure

### No

- **Customer Org.:**
  - Cust 1
  - Cust 2
  - Cust 3
  - Cust 4

- **Leveraging System:**
  - Identity Management Service
  - Leveraging SaaS A
  - Leveraging SaaS B

- **Leveraged System:**
  - IaaS
  - IaaS

**External Service or Interconnection**

Interconnections or External Services are not leveraged authorizations
- Even if they have an authorization
- SaaS A handles the Identity Management Service as a system component

OSCAL supports this, just not as a L.A.
Authorization-to-Use: OSCAL Support

Scenario 1: OSCAL SSP / With Access
The leveraged system is using an OSCAL SSP; and the leveraging system is permitted to access it.
No CRM/SSRM is needed.
Preferred approach!

Scenario 2: OSCAL SSP / No Access
The leveraged system is using an OSCAL SSP; however, the leveraging system is not permitted to access it.
An OSCAL CRM/SSRM is used.
Typical FedRAMP Scenario

Scenario 3: Legacy SSP
A leveraged system is still using a legacy SSP.
A legacy Customer Responsibility Matrix (CRM) or System Security Responsibility Matrix (SSRM) are used/available.
Transition scenario for an imperfect world

Completed

Post OSCAL 1.0.0

Three Scenarios
OSCAL content is for tools to consume!

Humans can see the information in nice html or pdf format using simple transformations over OSCAL content.

Example OSCAL Catalog transformed to HTML:
https://github.com/usnistgov/oscal-tools/blob/master/xslt/publish/generic-preview/oscal_catalog_html.xsl
Publicly Available Resources

Documentation:
Catalog, Profile, Component, SSP, SAP, SAR, POA&M:
https://pages.nist.gov/OSCAL/documentation/

Example:
Generic examples:
https://github.com/usnistgov/oscal-content/tree/master/examples
NIST SP 800-53 R4 and Rev5 catalog and baselines (XML & JSON):
https://github.com/usnistgov/oscal-content/tree/master/nist.gov/SP800-53

FedRAMP Automation:
Repository (FedRAMP catalog and baselines (XML & JSON) included):
https://github.com/GSA/fedramp-automation
https://www.fedramp.gov/using-the-fedramp-oscal-resources-and-templates/

Tools
OSCAL Java Library: https://github.com/usnistgov/liboscal-java
XSLT Tooling: https://github.com/usnistgov/oscal-tools/tree/master/xslt
OSCAL Kit: https://github.com/docker/oscalkit
OSCAL GUI: https://github.com/brianrdfsa/OSCAL-GUI

Please visit: OSCAL Club:oscal-club/awesome-oscal:
https://github.com/oscal-club/awesome-oscal
OSCAL Adopters

- FedRAMP
- Noblis
- HHS CMS
- National Renewable Energy Lab
- GovReady
- C2 Labs
- cFocus Software
- Shujinko
- Robers Bosch (EU|Germany)
- Telos

- Booz Allen Hamilton
- AWS
- Microsoft
- Coalfire
- Kratos
- eMASS
- CSAM
- Volant Associates, LLC
- Salesforce
- Oracle
Questions?

Contact us at: oscal@nist.gov
Chat with us on Gitter: https://gitter.im/usnistgov-OSCAL/Lobby
Collaborate with us on GitHub: https://github.com/usnistgov/OSCAL
Join our COI meetings: https://pages.nist.gov/OSCAL/contribute/#community-meetings

Thank you!