Open Security Controls Assessment Language

What is OSCAL and Who Needs It?

Lecture #1
Presenter: Dr. Michaela Iorga
NIST OSCAL Strategic Director
NIST is hosting a series of monthly educational lectures and workshops, scheduled on the third Tuesday of each month, 11:00-12:00 EST.

Purpose: improve OSCAL adoption by expanding the OSCAL community of interest (COI) through the onboarding of members who have no previous knowledge of OSCAL.

Compliance = the act of conforming to a set of standards, regulations, or requirements.

Compliance Components:

- **Regulatory compliance**: the actions an organization takes to comply with applicable external laws, regulations, and guidelines.
- **Corporate compliance**: the actions an organization takes to comply with internal policies and procedures, in addition to external regulations.

Risk Management = the process of identifying, assessing, and managing potential threats that could damage the organization’s reputation and earnings.

Despite the differences between compliance and risk management, the right risk management technology can actually address both.
Compliance & Risk Management Are Hard!

Information technology is complex & calls for automation

DevOps & IaC is hard in multi-clouds & Calls for interoperability & standardization

Regulatory frameworks are burdensome & Need interop auto GRC tools

Risk management is hard & Experts need automation

Paper-based A&A doesn’t scale & Calls for auto updates

Security vulnerabilities are everywhere & Calls for auto updates

Before the audit

During the audit

After the audit
Tools

OSCAL sets the foundation for automation and interoperability.

A (Cyber) Machine-readable Esperanto that enables actors, 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
What is OSCAL?

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.
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.
The following outline is a representation of the content in the combination of all OSCAL models. For each element or corresponding entry in the XML Format Reference, the cardinality and data type are also provided for each element or attribute.

```
<catalog uuid='uid' [1]
  > <metadata ... /></metadata> [1]
  > <param id='token' class='token' depends-on='token'> ... </param> [0 to 1]
  > <control id='token' class='token'> ... </control> [0 to 1]
  > <group id='token' class='token'> ... </group> [0 to 1]
  > <back-matter> ... </back-matter> [0 or 1]
</catalog>
```

```
<component-definition uuid='uid' [1]
  > <import-component-definition href='uri-reference'/ > [0 to 1]
  > <capability uuid='uid' name='string'> ... </capability> [0 to 1]
</component-definition>
```

```
<system-security-plan uuid='uid' [1]
  > <assessment-plan ... /></assessment-plan> [1]
```
OSCAL Models’ References

The following is the XML format reference for the combination of all OSCAL models, which is organized hierarchically. Each entry represents the corresponding XML element or attribute in the model’s XML format, and provides details about the semantics and use of the element or attribute. The XML Format Outline provides a streamlined, hierarchical representation of this model’s XML format which can be used along with this reference to better understand the XML representation of this model.

**XML NameSpace**: http://scrs.nist.gov/ns/oscal/1.0

This format represents a combination of all the OSCAL models.

---

The following is the JSON format reference for the combination of all OSCAL models, which is organized hierarchically. Each entry represents the corresponding JSON property in the model’s JSON format, and provides details about the semantics and use of the element or attribute. The JSON Format Outline provides a streamlined, hierarchical representation of this model’s JSON format which can be used along with this reference to better understand the JSON representation of this model.

**JSON Base URI**: http://scrs.nist.gov/ns/oscal/1.0

This format represents a combination of all the OSCAL models.
OSCAL Releases and News

OSCAL 1.0.0
RELEASED ON JUNE 7, 2021
LATEST: OSCAL 1.0.4

“...First official, major release of OSCAL provides a stable OSCAL 1.0.0 for wide-scale implementation ...”

Latest OSCAL patch release: 1.0.4 (backwards compatible) fixes s bug.

https://github.com/usnistgov/OSCAL/releases
OSCAL Content Maintained by NIST

https://github.com/usnistgov/oscal-content
OSCAL Models >>> OSCAL Content >>> OSCAL Tools

OSCAL Models
- OSCAL Models
- OSCAL Content
- OSCAL Tools

OSCAL Editorial Tools
- OSCAL Models
- OSCAL Content
- OSCAL Tools

OSCAL GRC Tools
- OSCAL Models
- OSCAL Content
- OSCAL Tools

800-53 in OSCAL
- CCM 4.0 in OSCAL
- CIS v8 in OSCAL
- 800-53 SSP
- CCM 4 SSP
- 800-53+CMM SSP
- 800-53 AP/AR/POA&M
- CCM 4 AP/AR/POA&M
- 800-53+CCM AP/AR/POA&M

https://github.com/usnistgov/OSCAL
https://github.com/usnistgov/oscal-content
https://github.com/usnistgov/oscal-tools
<xml version="1.0" encoding="UTF-8" standalone="yes">
  <controls-control>
    <family>ACCESS CONTROL</family>
    <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
    <priority>PI</priority>
    <baseline-impact>LOW</baseline-impact>
    <statement>
      <description>The organization identifies, develops, documents and disseminates to relevant personnel the access control policy or policies. The policy includes the organization's definition of access control, how access is granted and reviewed, and the format for documenting and disseminating the policy. The organization documents and disseminates the policy in multiple formats for all relevant personnel. The organization shall review and update the policy at least annually. The policy is reviewed by the organization's leadership. The policy is provided to relevant personnel and documented in a format that can be searched. The policy is also documented in a format that can be searched.
    </statement>
  </controls-control>
</xml>
What can you do with the OSCAL models?
Who Can Benefit & How?

Risk Management & OSCAL content

Actors
- Product Engineer
- Component Supplier
- Solution Evaluator
- Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

RMF steps: PREPARE CATEGORIZE SELECT IMPLEMENT ASSESS AUTHORIZE CON-MON

OSCAL Catalog
- Source
- Link
- OSCAL Profile
- Link
- OSCAL Component Definitions
- Source
- Link
- OSCAL System Security Plan
- Link
- OSCAL Assessment Plans
- Transfer
- OSCAL Assessment Results
- Transfer
- OSCAL POAM
- Transfer
- Authorization (ATO)
- OSCAL Plan of Actions & Milestones

OSCAL Catalog Creators
- System
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System
- System Engineer
- System Operator
- Product Engineer
- Component Supplier
- Solution Evaluator
- Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

OSCAL Solution Evaluator
- Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Component Supplier
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Authorizing Official

System Engineer
- System Operator

System Operator

Product Engineer
- Component Supplier
- Solution Evaluator
- Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Component Supplier
- Solution Evaluator
- Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Solution Evaluator
- Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Authorizing Official

System Engineer
- System Operator

System Operator

OSCAL Creators
- Catalog Creators
- System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Architect
- System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Engineer
- System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

System Owner
- Auditor
- Assessor
- System Operator
- System Owner
- Authorizing Official
- System Engineer
- System Operator

Authorizing Official

System Engineer
- System Operator

System Operator

Who Can Benefit & How?
OSCAL is a community-driven program! Please join us!

Thank you!

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

https://www.nist.gov/OSCAL
Open Floor Discussion

Ground Rules of Engagement

- Keep the discussion respectful by:
  - using welcoming and inclusive language
  - being respectful of differing viewpoints and experiences
  - gracefully accepting constructive criticism
  - wait for one speaker to finish before speaking

- Speak from your own experience instead of generalizing.

- Do not be afraid to respectfully challenge one another by asking questions focused on ideas not on the company or presenter.

- The final goal is not to always agree but rather gain a deeper understanding.