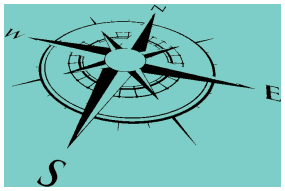
About OSCAL

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... Control-based information expressed using OSCAL formats allows you to:

- Easily access control information from security and privacy control catalogs
- Establish and share machine-readable control baselines
- Maintain and share actionable, up-to-date information about how controls are implemented in your systems
- Automate the monitoring and assessment of your system control implementation effectiveness

Automated Control-Based Assessment Supporting Control-Based Risk Management with Standardized Formats — NIST is developing the Open Security Controls Assessment Language (OSCAL) as a standardized, data-centric framework that can be applied to an information system for documenting and assessing its security controls. Today, security controls and control baselines are represented in proprietary formats, requiring data conversion and manual effort to describe their implementation. An important goal of OSCAL is to move the security controls and control baselines from a text-based and manual approach (using word processors or spreadsheets) to a set of standardized and machine-readable formats.

Contents



National Institute of Standards and Technology (NIST)

Stakeholder(s):

Security Professionals :

You are responsible for documenting security controls and how they are applied within a system. — With systems security information represented in OSCAL, security professionals will be able to automate security assessment, auditing, and continuous monitoring processes... There are a number of complicating factors contributing to the challenges faced by information system security professionals today.

- *Multiple regulatory standards and frameworks, which change over time;*
- *Regulatory standards and frameworks overlap in scope and can often conflict or be difficult to manage together; and*
- *Information systems are increasing in size and complexity.*

To address information security and privacy risks, the implementation of selected controls need to be verified and shown to be effective. To provide assurance of a system's security and privacy posture, the control implementation of a system must be both correctly described, assessed, and authorized. These tasks are resource-intensive, and often challenging to perform within budget constraints given the complexity of the problem. The standardized formats provided by the OSCAL project help to streamline and standardize the processes of documenting, implementing and assessing security controls. The automation enabled by the OSCAL formats will reduce complexity, decrease implementation costs, and enable the simultaneous, continuous assessment of a system's security against multiple sets of requirements. Additionally, paperwork will be significantly reduced.

Security-Related Information Assessors :

You are responsible for assessing security-related information produced by others.

Security-Related Tool Developers :

You build tools and utilities to help other players, enabling them to do more work more consistently, thoroughly, accurately and easily.

Policy Authors :

You write policy documents (catalogs or profiles/baselines/overlays) defining, characterizing and customizing security controls for others to use.

Vision

Standardized and machine-readable security controls

Mission

To provide security control information in machine-readable formats.

Values

Data-Centricity: Transitions the legacy approach to security plan generation and management (Word and Excel documents) to a data-centric approach based on common data standards such as XML/JSON.

Extensibility: Puts security compliance data to work by allowing an extensible architecture that expresses security controls in both machine and human readable formats.

Integration: Allows tool developers to implement APIs and provide a standards-based foundation for next generation compliance tools.

Automation: Apply the benefits of the data-centric approach to automate existing processes that are resource intensive.

Principles: OSCAL Design Principles -- To address these goals, the OSCAL project is guided by the following design principles.

Interoperability: Interoperable Data Formats -- Produce a set of interoperable, extensible, machine-readable formats through a community-focused effort that supports a broad range of control-based risk management processes.

Translation: Provide XML-, JSON-, and YAML-based formats that allow for lossless translations between XML, JSON, and YAML representations.

Identification: Provide a common means to identify and version shared resources.

Standardization: Standardize the expression of assessment artifacts, driving crowd-sourced development and improvement across profile and implementation layers.

Relevance: Be Relevant Now, Enable a Better Future -- Align OSCAL models with current, practical information, and support advanced structures that provide for greater automation and verification.

Traceability: Ensure security controls, implementation, and assessment processes have full traceability to the selected control baseline and across system boundaries for interconnected systems and common control providers.

Adoption: Provide a path for early adoption and ongoing evolution around how OSCAL will be used.

Evolution

1. Paperwork

Decrease Paperwork

Stakeholder(s)

Information Security Professionals

Information Security Vendors

Drive a large decrease in the paperwork burden for both information security professionals and vendors.

1.1. Catalogs, Frameworks & Information

Normalize the representation of security control catalogs, regulatory frameworks, and system information using precise, machine readable formats.

1.2. Information Sharing

Allow the sharing of control implementation information across communities.

2. Security Assessments

Improve System Security Assessments

Improve the efficiency, accuracy, and consistency of system security assessments.

2.1. Requirements & Traceability

Assess a system's security control implementation against several sets of requirements simultaneously and ensure traceability between the requirements.

2.2. Consistency

Enable assessments to be performed consistently, regardless of system type.

3. Continuity

Enable Continuous Assessment

Allow a system's security state to be assessed more often, ideally continuously, driving continuous assurance.

3.1. Labor & Time

Drive a large decrease in assessment-related labor, decreasing assessment and authorization time.

3.2. Effectiveness

Support the assessment of control implementation effectiveness based on data collected using a continuous monitoring capability.

Administrative Information

Start Date: 2020-06-03
End Date:

Publication Date: **2020-06-29**
Source: https://pages.nist.gov/OSCAL/

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: