# NIST Cybersecurity White Paper
# NIST CSWP 53 ipd

# Charting the Course for NIST OSCAL

Initial Public Draft

Michaela Iorga
Marilyn Nguyen
*Computer Security Division*
*Information Technology Laboratory*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.53.ipd

December 2, 2025

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.



**Publication History**
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

**How to Cite this NIST Technical Series Publication**
Iorga M, Nguyen M (2025) Charting the Course for NIST OSCAL. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 53 ipd.
https://doi.org/10.6028/NIST.CSWP.53.ipd

**Author ORCID iDs**
Michaela Iorga: 0000-0001-7880-6045
Marilyn Nguyen: 0009-0004-1186-5613

**Comment Period**
December 2, 2025 – January 13, 2026

**Submit Comments**
oscal@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

**Additional Information**
Additional information about this publication is available at https://csrc.nist.gov/publications/cswp, including related content, potential updates, and document history.

## Abstract

This document introduces the Open Security Controls Assessment Language (OSCAL), a NIST-developed, open-source, machine-readable language that modernizes manual, paper-based cybersecurity compliance by enabling automated and scalable processes. OSCAL standardizes security documentation for easier monitoring and risk management across different tools. It can also be extended and integrated with numerous capabilities, including software supply chain standards using OSCAL SBOMs, digital twin technology and AI-driven compliance. Overall, OSCAL helps organizations improve efficiency, accuracy, and collaboration in cybersecurity.

## Keywords

Agentic AI; compliance; continuous assessment; digital twins; interoperability; machine-readable formats; Open Security Controls Assessment Language; OSCAL; risk management; security automation.

## Table of Contents



## List of Tables



## List of Figures

## Acknowledgments

*This white paper is dedicated to our colleague and friend, Kathy Ton-Nu, whose warmth, kindness, and dedication will be remembered always.*

The authors gratefully acknowledge the insightful guidance provided by Dr. Sanjay (Jay) Rekhi and extend thanks to their colleagues Isabell Van Wyk, Nedim Goren, Dmitry Cousin, Selena Xiao and Jim Foti for their valuable feedback and constructive suggestions. Appreciation is also extended to all other reviewers, members of the OSCAL community, whose expertise, collaboration, and support contributed to the completion of this work.

## 1. Introduction

In a digital world defined by rapid cloud adoption, intricate system dependencies, and evolving threats, the traditional and proprietary methods of cybersecurity compliance methods no longer scale effectively. The burden of paper-based documentation, manual assessments, and proprietary tools limits security data portability. As systems have evolved, the complexity of this work has increased significantly, and understanding interdependencies, control inheritance, and risk mitigation across layered systems is a monumental task.

To address these challenges, the National Institute of Standards and Technology (NIST) has collaborated with industry partners to develop the Open Security Controls Assessment Language (OSCAL) [1], which is an open-source, machine-readable language designed to digitize security information and support dynamic risk management. This solution supports fast, cost-effective, accurate, and continuous assessments and monitoring of critical systems. It also meets the urgent need for standardized, machine-readable documentation and portable, automated compliance processes.

Developed with flexibility and operational excellence at its core, OSCAL began as a federal-focused project but has quickly grown into a global initiative. It enables the shift from manual to machine-driven, continuous assessments for a broad range of compliance domains. OSCAL's rapid international adoption includes collaborations with organizations from the information technology industry and span multiple vertical markets, including international governments, public sectors, and financial services. Its use cases in privacy, safety, and accessibility across a variety of regulatory frameworks highlights its groundbreaking role in advancing proactive system resilience assessments.

## 2. The OSCAL Ecosystem

OSCAL is a community-driven initiative to standardize and automate security assessments and risk management processes. The OSCAL ecosystem features a broad network of government agencies, private-sector vendors, open-source contributors, and standards bodies working together to advance and mature the language. This ecosystem relies on key resources in several categories, as shown in Fig. 1:

- **OSCAL models/schemas [2]:** Define the structure of the language, and provide a standardized framework for continuous risk management
- **Content (OSCAL artifacts) [3]:** Standardized digital representations of information that support risk management processes (e.g., requirement, controls, safeguards), including their selection, implementation, and continuous assessment
- **Editorial tools [4]:** Support the creation, editing, and management of OSCAL content
- **GRC (governance, risk, and compliance) tools:** Enable the practical application and use of OSCAL to offer a consistent format for describing security requirements
- **Operationalized content:** Automated DevOps processes, such as continuous integration and continuous deployment (CI/CD) pipelines that leverage OSCAL's native traceability and updatability (e.g., change management through granular unique identifiers systems)**.**

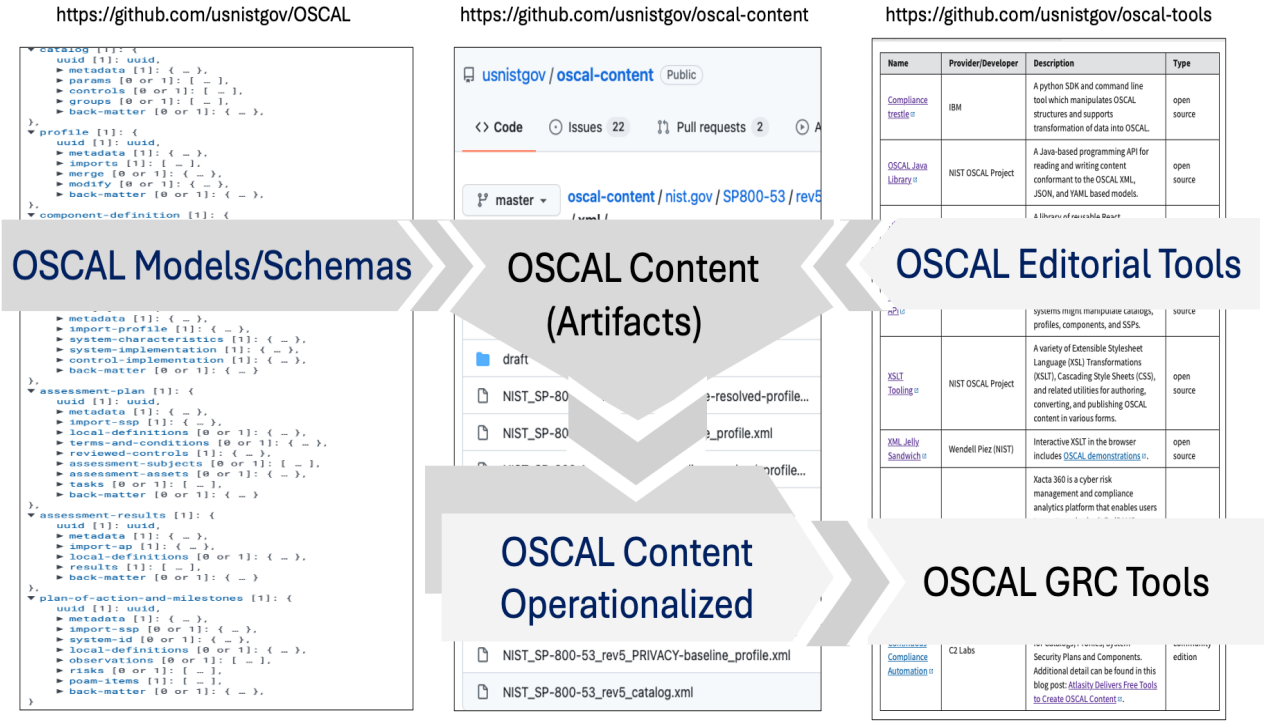


**Fig. 1. OSCAL Ecosystem Diagram**

As the official owner and primary authority responsible for OSCAL, NIST leads the development and maintenance of the OSCAL models/schemas, which form the structure of the framework. In addition, NIST produces OSCAL content, including foundational artifacts that support implementation across a variety of use cases. In Fig. 1, the darker gray boxes represent NIST's primary responsibilities in the OSCAL ecosystem. This content is made freely available as open-source resources to promote accessibility and adoption.

While NIST retains ownership and governance over OSCAL, it actively promotes a collaborative, community-driven model that encourages contributions from other organizations, including the following key stakeholders:

- **Guideline/regulatory authors:** Entities responsible for creating and publishing regulatory documents, such as policies, control catalogs, profiles, baselines, and overlays. These actors define, customize, and tailor requirements and controls to guide organizations in managing cybersecurity risks.
- **Security professionals:** Entities responsible for documenting the implementation of requirements or controls and demonstrating their effectiveness within information systems. They ensure that safeguards (i.e., implemented controls) are properly applied and meet required standards to mitigate identified risks.
- **Assessors/auditors:** Independent entities responsible for evaluating the claimed satisfaction of requirements or control implementation to determine whether systems meet the risk management objectives of system owners or authorizing officials. This role involves analyzing documentation, verifying implementation, and identifying gaps or vulnerabilities.
- **Tool developers:** Entities that develop editorial or GRC tools that automate and streamline risk management processes to improve efficiency and precision. Such tools empower security teams to perform their tasks more effectively and at scale.

These participants generate content, develop tools, and operationalize use across systems. Their expertise is essential to advancing the maturity of the language and preparing it for international standardization. Any proposed changes to OSCAL or OSCAL-related content must be transparently reviewed and vetted by the community before being adopted or implemented by NIST.

Two essential tool categories in the ecosystem are crucial to the success and global adoption of OSCAL: editorial tools and GRC tools. Editorial tools support the generation, editing, and management of OSCAL content. GRC tools, which can be developed by vendors, then operationalize that content by integrating it into real-world workflows, enabling automation, and supporting security assessments and compliance reporting. Without editorial tools, creating and maintaining content would not be possible. Without GRC tools, that content would remain static and unusable in practice. Together, they enable organizations to fully utilize and accomplish the benefits of security automation and standardized compliance.

The OSCAL community is also strengthened by a wide range of supporters, such as the OSCAL Foundation [5], which was established in January 2025 as an industry-led consortium. The

Foundation focuses on key areas to accelerate growth, maturation, and adoption, including content generation, model maturation, and community-consensus building. Specifically, it is working to achieve six core objectives: adoption, education, community engagement, development, extension, and internationalization.

## 3. OSCAL as the Shipping Container of Cybersecurity

To better understand how OSCAL streamlines complex security processes, compare it to something familiar: a shipping container. Historically, transporting goods by sea was time-consuming, extensive, and labor-intensive. The introduction of standardized shipping container sizes in 1956 dramatically changed the industry by maximizing the use of space, simplifying transfers, speeding up loading and unloading operations, and reducing shipping costs.

Before container standardization, every shipment required custom handling. Today, cybersecurity documentation faces a similar challenge. Documents are often created in a range of formats that require manual restructuring before being shared or reused across systems. OSCAL solves this by introducing a common, machine-readable format — just like the standardized shipping container — that makes it easier to store, transfer, and automate compliance data across platforms and organizations.

OSCAL enables:

- Vendors to document the security controls implemented in their products
- System owners or policy makers to define standardized “playbooks” for system components
- System owners to test, review, and provisionally authorize system components
- The reuse of authorized components across different systems
- Streamlined documentation generation to automate the traditionally manual and human-intensive labor of generating system security plans (SSPs)

OSCAL’s implementation layer divides systems into modular components that can be reassembled or evaluated based on different needs, such as functionality or role. Think of OSCAL as “**documentation as code**” or “**compliance as code**,” which is essentially the digital equivalent of standardizing shipping containers. It is designed to carry security information about controls, baselines, their implementation, and assessments, and it enables DevOps-style automation in the traditionally manual world of security governance.

### 3.1. OSCAL’s Layered Architecture and Models

OSCAL is organized into multiple **layers**, each containing specific **models** that serve distinct operational purposes and roles. Each model defines structured ways to represent how data is organized, known as information structures. Together, these structures form an information model, which is bound to multiple serialization formats, such as XML, JSON, and YAML. These serialization formats represent a concrete data model that specifies how an OSCAL information model is represented. Although the syntax of each format differs, all formats for a given model represent the exact same information. This means that **OSCAL content** that is written in one supported format (i.e., XML, JSON, or YAML) can be translated into any of the other formats without data loss.

The NIST OSCAL website offers an overview of the OSCAL project, including resources, tutorials, detailed documentation, workshops, references, downloads, and more to support users at every level. The OSCAL specification is maintained in a live versioned format.

Current OSCAL **layers** and released **models** are:

- **Control Layer**
  - Catalog Model
  - Profile Model
- **Implementation Layer**
  - Component Definition Model
  - System Security Plan (SSP) Model
- **Assessment Layer**
  - Assessment Plan Model
  - Assessment Results Model
  - Plan of Action and Milestones (POA&M) Model

In addition to the currently released OSCAL models, NIST is working with community members to expand OSCAL's capabilities through new models, such as the Control Mapping Model and Shared Responsibility Model.

The OSCAL schemas, which define the "language" of OSCAL, are publicly hosted on the OSCAL GitHub Repository.[1] Community members are encouraged to participate by forking the repository, making improvements, and submitting pull requests to contribute to the ongoing development of OSCAL.

NIST also publishes key cybersecurity documents in OSCAL, including the Cybersecurity Framework v2.0 [6], NIST Special Publication (SP) 800-53 [7], SP 800-53B [8], and 800-53A [9], NIST Special Publication (SP) 800-171 [10] and NIST Special Publication (SP) 800-218 [11]. These OSCAL artifacts contain structured sets of requirements and are maintained on the public OSCAL Content Repository. NIST OSCAL team will continue to work on converting more NIST special publications of interest to our community.

### 3.2. The OSCAL Advantage: Standardized Efficiency and Interoperability

By automating documentation, assessments, and risk tracking, OSCAL addresses numerous real-world challenges, including:

- Faster, cheaper, and more accurate audits
- Tool interoperability and reduced vendor lock-in

[1] Additional OSCAL-related GitHub repositories are also available on NIST's GitHub enterprise, though they are not covered in this document.

- Reuse of common controls and scalability across environments
- Automated validation and continuous monitoring

In addition to its core capabilities, OSCAL offers an open, machine-readable set of formats in XML, JSON, and YAML that make it easier to integrate into existing workflows and empower organizations to:

- Digitize and automate compliance documentation
- Accelerate audits and Authority to Operate (ATO) processes
- Reduce errors and manual effort
- Improve efficiency and consistency across security and compliance activities

OSCAL defines a comprehensive ecosystem of digital artifacts, including control catalogs and profiles, SSPs, component definitions, and assessment plans and results. This ecosystem delivers unprecedented transparency throughout the compliance life cycle and helps organizations manage and demonstrate their security posture with greater confidence and clarity.

## 4. Global Momentum and the OSCAL Foundation: Scaling the Mission

NIST collaborated with industry contributors to launch the OSCAL Foundation [5], which is a nonprofit organization dedicated to:

- Promoting **adoption and education**
- Facilitating **community collaboration**
- Supporting **development, tooling, and global standardization**

The Foundation's mission is to help organizations transition from manual, paper-based compliance processes to automated, accurate, and future-ready frameworks using OSCAL. To guide this effort, NIST has encouraged the OSCAL community to establish a framework that aligns various stakeholder interests while preserving OSCAL's openness and flexibility. Thanks to its open design, OSCAL has gained support from federal agencies, the governments in Australia and Singapore, and major tech leaders like IBM/Red Hat [12], Google [13], AWS [14]. NIST expects the OSCAL Foundation to serve as a key channel for community contributions and ensure that OSCAL evolves to meet the needs of adopters worldwide.

Figure 2 illustrates the Foundation's contributions workflow, which similarly applies to contributions from other stakeholders and OSCAL-related repositories.

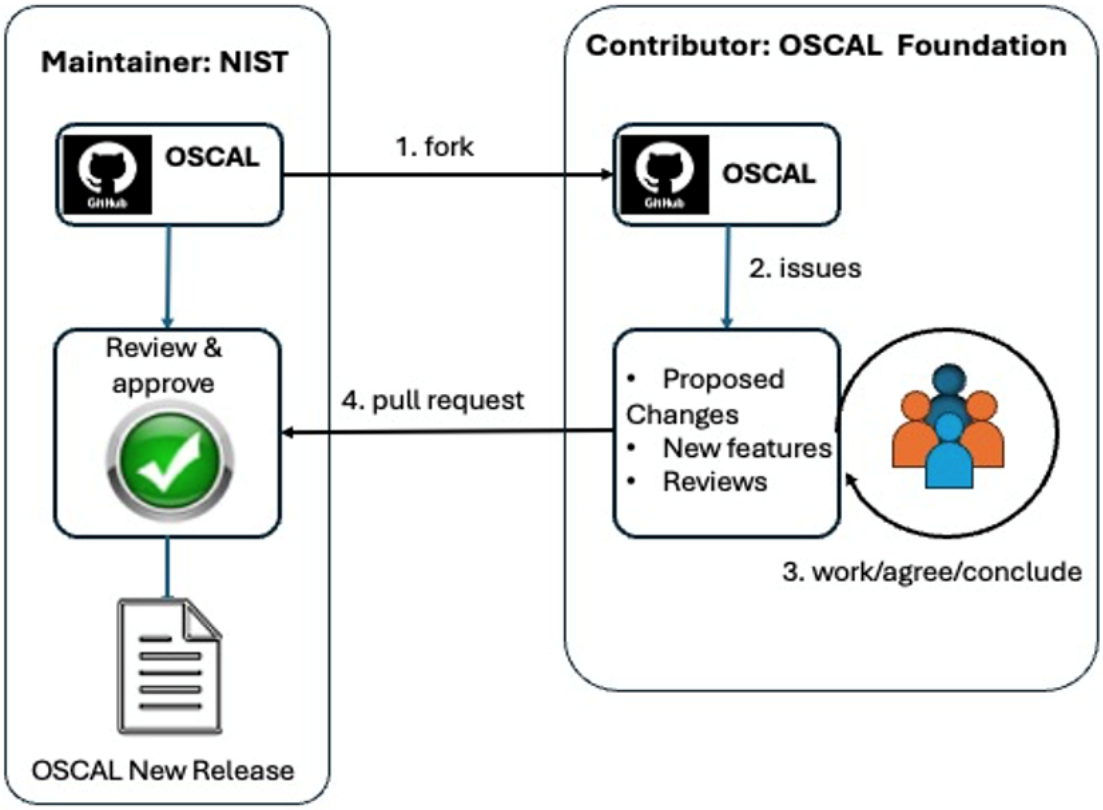


**Fig. 2. OSCAL Foundation contribution workflow**

# 5. Beyond Control Assessments: Augmenting and Integrating Capabilities

## 5.1. OSCAL and Software Bills of Materials: A Natural Fit

In addition to efforts regarding security and compliance documentation, OSCAL is also advancing software supply chain transparency. Its component definition model complements Software Bills of Materials (SBOMs), which track software component origins and vulnerabilities. The model enables the direct mapping of software elements to relevant security and privacy controls, thus improving the creation and maintenance of artifacts like SSPs.

Today, experts primarily rely on two SBOM standards:

1. **CyloneDX** - a "standard that provides advanced supply chain capabilities for cyber risk reduction. CycloneDX is a lightweight software bill of materials (SBOM) standard designed for use in application security contexts and supply chain component analysis" (source) [OWASP Foundation][15], and
2. **Software Package Data Exchange (SPDX)** - an "open standard for communicating software bill of materials information, including provenance, license, security, and other related information. SPDX reduces redundant work by providing common formats for organizations and communities to share important data…" (source) [Linux Foundation Project][16].

CycloneDX is more lightweight and is often favored for vulnerabilities and supply chain risk analysis due to its streamlined format, while SPDX is favored for its depth in license compliance and software package information. Table 1T shows how OSCAL's data objects align with those of CycloneDX and SPDX.

**Table 1. Alignment of OSCAL data objects with SPDX and CycloneDX**

| Data Type | SPDX | CycloneDX | OSCAL |
|---|---|---|---|
| Software component metadata | ✅ | ✅ | ✅ (non-native) |
| Licenses and legal information | ✅ | ✅ | ❌ |
| Package relationships (dependencies) | ✅ | ✅ | ✅ (non-native) |
| Vulnerability information | Limited | ✅ | ✅ |
| Security controls | ❌ | Limited | ✅ |
| Provenance & trust (e.g., hashes) | ✅ | ✅ | ✅ |
| Cryptographic elements (signature) | ✅ (optional) | ✅ | ✅ |

Using OSCAL, organizations can create artifacts that document cryptographic elements, provenance, implemented security controls, and known vulnerabilities of a software component. These OSCAL artifacts can then be connected to any chosen SBOM using OSCAL's built-in extension mechanisms. Fig. 3 illustrates these linking mechanisms using the Component Definition outline.

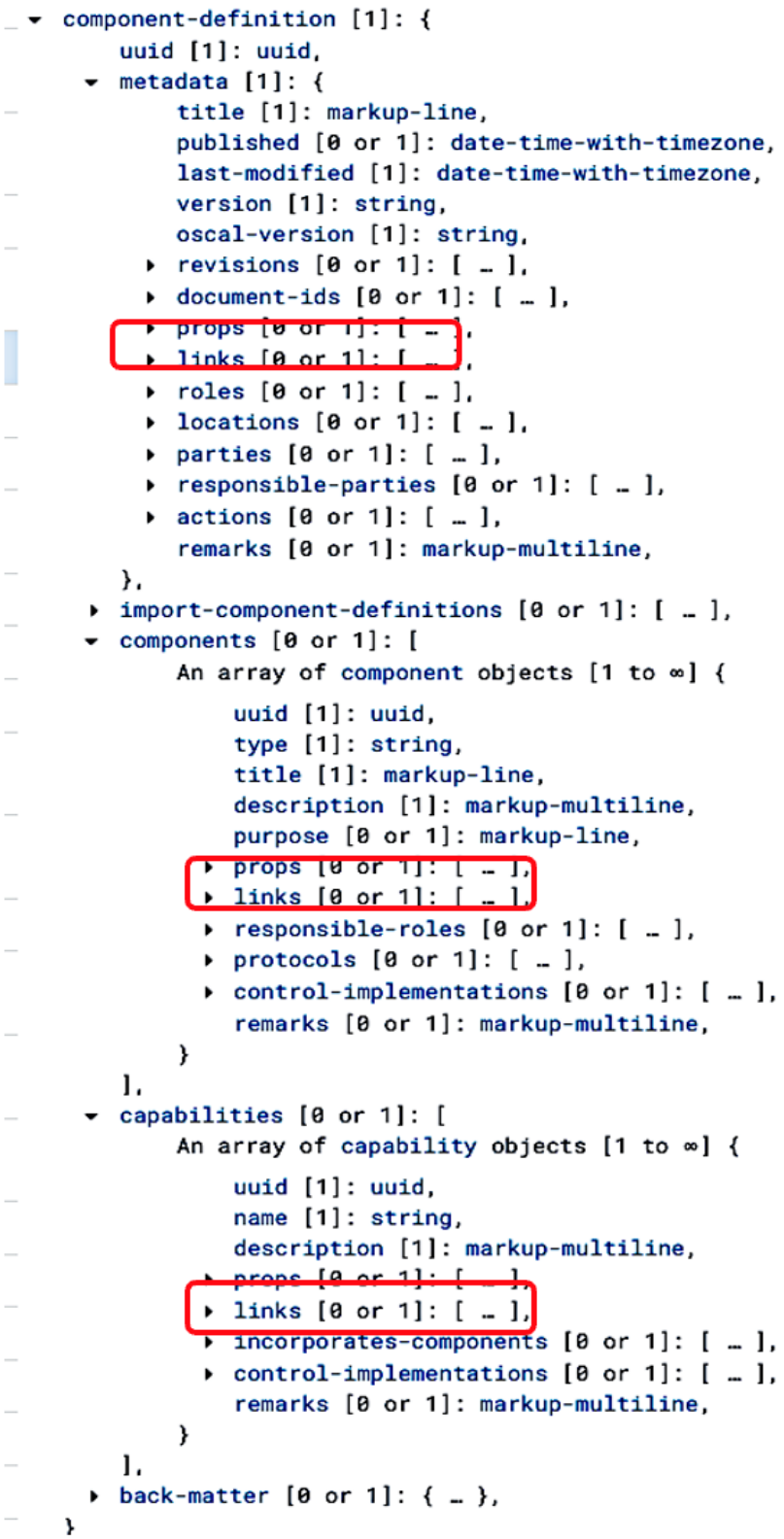


**Fig. 3. OSCAL component definition outline**

Together, the OSCAL and SBOMs provide comprehensive visibility into software components, support proactive risk management, and streamline the process of identifying and responding to vulnerabilities. This combination empowers organizations to strengthen their security posture across complex technology environments.

## 5.2. Elevating Assessment Automation: The Power of OSCAL and Emerging Technologies

The digitization of security documentation through OSCAL provides a strong foundation for next-generation technologies that are revolutionizing how we understand, simulate, and secure complex systems, such as digital twins, agentic AI, and generative AI.

Digital twin technology enables the creation of electronic representations of real-world entities and the ability to visualize their states and transitions. A system's digital twin is a dynamic, data-rich virtual model capable of reflecting its security and compliance posture, tracking transitions between operational states (including update outcomes), and even simulating the system's response to advanced persistent threats and vulnerability exploits as part of the system's resilience assessment and review.

Traditional security plans are static paper-based documents with limited utility, even when ingested into GRC platforms, because they are architected for human-oriented data processing and representation rather than machine interpretation and processing. OSCAL overcomes this limitation by converting these documents into machine-readable artifacts that can be continuously updated. These "living documents" provide the structured data required for AI systems to operate effectively.

### 5.2.1. From Static Security Artifacts to Intelligent Digital Twins

NIST Interagency Report (IR) 8356 [17] defines a digital twin as a "virtual representation of real-world entities and processes synchronized at a specific frequency and fidelity." The report also emphasizes the importance of a digital twin definition, described as a "machine-readable specification that describes features that may be modeled for a particular type of real-world entity." In other words, a *digital twin definition* refers to a *class* or *type* of entity rather than a specific instance. It outlines which features of that entity type can be modeled (both statically and dynamically), how those features are digitally encoded and presented, and how they persist within a digital computing environment. Software applications can read these definitions to generate digital twin instances, which are virtual representations of actual physical objects that reflect their current and evolving states.

Extrapolating these concepts, the OSCAL SSP continuously updated through risk management processes, serves as the system's DNA and the foundation for its *digital twin definition* – the enabler of the system's digital twin. Just as a DNA sequence uniquely identifies an organism and provides the blueprint for its cloning, the OSCAL SSP provides a detailed, machine-readable DNA which serves as the blueprint of a system's digital twin. It captures the system's components, inventory, characteristics, controls, configurations, interconnections, protocols, and ports with fine granularity.

Once created, the digital twin can be continuously refined using assessment results that allow it to better reflect the system's real-time security and compliance postures. Plans of Actions and Milestones (POA&Ms) can also be developed and tested virtually on the digital twin before implementing changes in the live environment.


**Fig 4: Digital twin-based intelligent continuous system resilience management**

As Figure 4 graphically depicts, an AI-augmented digital twin would support data integration, simulation, prediction and optimization of system's functionality and its security capabilities.

Similarly, perceived or observed threats and exploit scenarios can be exercised against the digital twin to assess their impacts and better quantify the associated risks. Such simulation and analysis can be significantly enhanced through AI-augmented reasoning to provide deeper insights into system resilience and inform more effective risk mitigation strategies.

### 5.2.2. Autonomous Risk Reasoning with Agentic AI

Agentic AI refers to autonomous systems that are capable of goal-directed behavior, adaptive decision-making, and continuous unsupervised learning without human interaction. When combined with OSCAL data and digital twin technology, these AI agents function as intelligent and proactive risk management experts operating at machine speed and scale.

By integrating with OSCAL-formatted data and the system's digital twin, agentic AI can:

- Continuously monitor digital twins for compliance drift and detect deviations from expected control states,
- Identify configuration changes that affect control inheritance, particularly in complex environments like multi-tenant cloud systems,
- Map control dependencies to evaluate how vulnerabilities or policy changes propagate across interconnected systems, and

- Trigger assessments, generate POA&Ms, and propose mitigation strategies that adapt based on historical data and current risk profiles.

For example, an AI agent analyzing OSCAL assessment results might detect that a configuration change has invalidated the controls inherited from a cloud service provider. The AI agent would autonomously (i.e., without human input):

- Update the relevant assessment results,
- Generate new OSCAL POA&Ms,
- Notify stakeholders of the compliance drift,
- Recommend or even implement mitigation strategies,
- Update SSP and trigger a new assessment to confirm the efficacy of the mitigations.

In this architecture, as Fig. 5 depicts graphically below the information flow, AI agents evolve from passive monitoring tools into dynamic actors capable of maintaining compliance, improving system resilience, and reducing operational risk, thus accelerating the move toward autonomous cybersecurity ecosystems.

### 5.2.3. Generative AI: Simulating, Predicting, and Remediating

Generative AI models, including large language models like GPT, complement this autonomy by interpreting, synthesizing, and creating OSCAL content with high fidelity and speed. When paired with a system's digital twin, generative AI unlocks powerful, advanced capabilities, such as:

- Simulating "what-if" scenarios to evaluate the security or compliance impacts of architectural changes, vendor modifications, or policy shifts,
- Automatically generating OSCAL SSPs, assessment results, or POA&Ms, thus drastically reducing manual labor and improving consistency, or
- Creating tailored security narratives or executive summaries from OSCAL data and translating technical content into actionable, business-focused insights.

For example, generative AI can take OSCAL component definition artifacts for all components of a system and generate an accurate SSP, tailored policy-based recommendations, and a remediation plan based on the system's characteristics, data categorization, and inventory (see Fig. 5).

### 5.2.4. Real-Time Feedback Loops and Continuous Assurance

Agentic and generative AI augment digital twin technology to elevate OSCAL-driven automation from structured data management to intelligent, adaptive cybersecurity orchestration. This enables systems to not only document themselves, but reason, react, and improve in real-time. Organizations can then achieve continuous authorization through:

- Real-time feedback loops that connect ongoing assessments directly with the current system state,
- Near real-time scoring and benchmarking to identify risks and drive continuous improvements.

These integrated technologies and OSCAL's continuous self-healing process (see Fig. 5) provide auto-immunization for systems architected with core resilience.

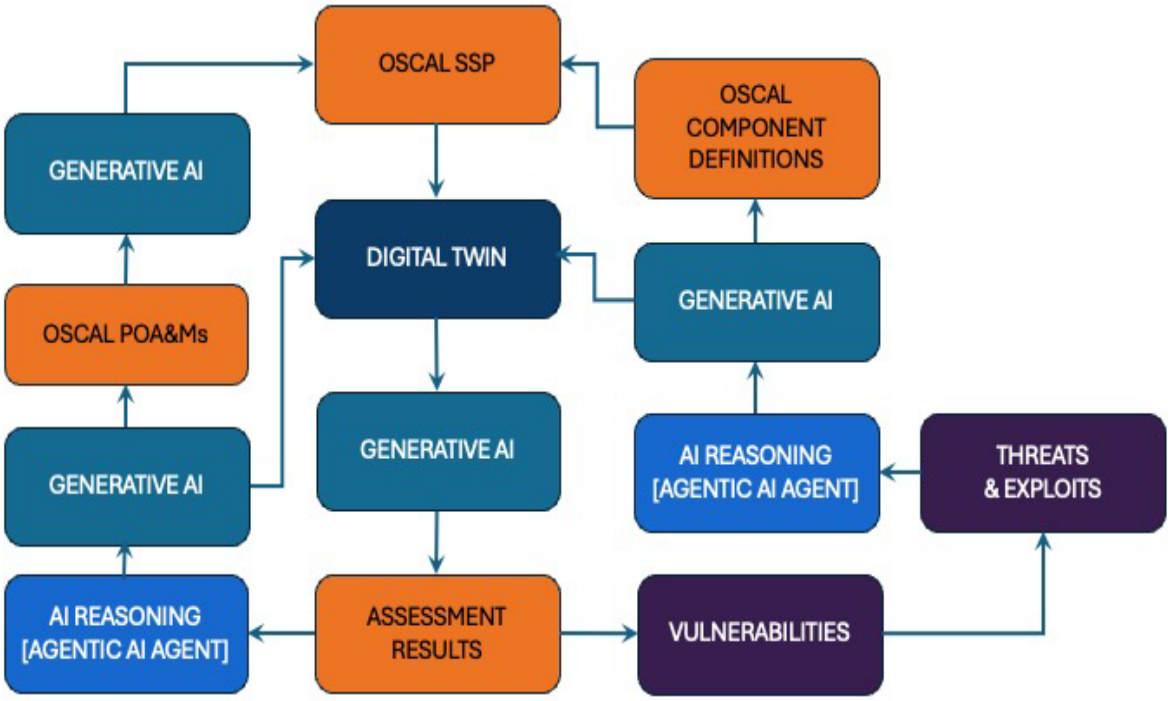


**Fig. 5. OSCAL's continuous self-healing process**

## 5.3. Federated and Scalable Intelligence

OSCAL's open, standardized formats simplify data sharing across teams and organizations. When paired with AI, this enables:

- Comparing security postures across multiple systems against industry benchmarks
- Federated learning in which AI models collectively improve threat detection and mitigation without exposing sensitive data

Together, these capabilities create scalable, collective intelligence that strengthens security across ecosystems, builds resilient systems from the bottom up, and strengthens national cybersecurity with comprehensive intelligent defense.

# 6. Why You Should "OSCAL-ize" Your Data

## 6.1. Join the OSCAL Community and Transform Compliance Together

By adopting OSCAL, organizations not only modernize their internal operations but also contribute to an open, forward-looking ecosystem that promotes innovation, reduces costs, and supports faster compliance outcomes. Now is the time to join a vibrant and collaborative community that is redefining how organizations approach security and compliance. Whether you are in the medical field managing sensitive patient data, part of the financial industry navigating stringent regulatory frameworks, or in the defense sector handling national security information, OSCAL provides the tools needed to operate with greater speed, accuracy, and interoperability.

Visit the OSCAL Monthly Workshops page to find information sessions hosted by experts and the OSCAL GitHub repository to connect with peers and guide the future of OSCAL.

## 6.2. Benefits of OSCAL Adoption

OSCAL offers a range of benefits for organizations seeking a more efficient, reliable, and scalable approach to security compliance, including:

1. Speed and Efficiency
    - Automated assessments slash compliance timelines
    - Standardized results reduce duplication and confusion
    - Faster ATO (Authority to Operate) cycles
2. Accuracy and Portability
    - Machine-readable formats reduce human error
    - Easy exchange between tools and platforms
    - Eliminates vendor lock-in through open standards
3. Total Ecosystem Interoperability
    - Enables integration with GRC platforms, scanners, monitoring tools
    - Supports continuous compliance and gap analysis
4. Scalability and Reusability
    - Common components and controls reused across systems
    - Inheritance models make shared responsibility clear in cloud environments

## 7. Final Thoughts: Build the Future of Compliance with OSCAL

OSCAL is more than just a standard. It is a catalyst for building intelligent, responsive, and resilient cybersecurity architectures. By integrating with digital transformation efforts and emerging technologies like agentic systems and generative AI, OSCAL drives the next evolution in proactive security and compliance.

OSCAL is also a growing, collaborative community dedicated to reshaping compliance for the modern era. Whether you are a policymaker, tool developer, auditor, or implementer, your insights and contributions are vital. The transformation is already underway. Join the OSCAL community and help shape the future of security and compliance.

## References

[1] National Institute of Standards and Technology (2025) OSCAL: the Open Security Controls Assessment Language. Available at https://pages.nist.gov/OSCAL/
[2] National Institute of Standards and Technology (2025) Layers and Models. Available at https://pages.nist.gov/OSCAL/learn/concepts/layer/
[3] OSCAL Content GitHub. Available at https://github.com/usnistgov/oscal-content/
[4] National Institute of Standards and Technology (2025) OSCAL Tools. Available at https://pages.nist.gov/OSCAL/resources/tools/
[5] The OSCAL Foundation (2025). Available at https://oscalfoundation.org
[6] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. Available at https://doi.org/10.6028/NIST.CSWP.29
[7] National Institute of Standards and Technology (2020) NIST SP 800-53 Rev. 5. Available at https://doi.org/10.6028/NIST.SP.800-53r5
[8] National Institute of Standards and Technology (2020) NIST SP 800-53B. Available at https://doi.org/10.6028/NIST.SP.800-53B
[9] National Institute of Standards and Technology (2022) NIST SP 800-53A Rev. 5. Available at https://doi.org/10.6028/NIST.SP.800-53Ar5
[10] National Institute of Standards and Technology (2024) NIST SP 800-171 Rev. 3. Available at https://doi.org/10.6028/NIST.SP.800-171r3
[11] National Institute of Standards and Technology (2022) NIST SP 800-218. Available at https://doi.org/10.6028/NIST.SP.800-218
[12] OSCAL Workshop (March 2025): "*OSCAL-based AI-augmented CISO Agent*". Talk available at https://pages.nist.gov/OSCAL/learn/presentations/mini-workshop/#:~:text=presentation%2C%20video%2C%20transcript-,2025/3/19,-11:00AM%2D12
[13] OSCAL Workshop (February 2023): "*Google's Internal OSCAL Adoption*". Talk available at https://pages.nist.gov/OSCAL/learn/presentations/mini-workshop/#:~:text=transcript%2C%20demo%20transcript-,2023/02/15,-11:00AM%2D12
[14] Michael Davie, January 2025. "*Using OSCAL to express Canadian cybersecurity requirements as compliance-as-code*". Available at https://aws.amazon.com/blogs/security/using-oscal-to-express-canadian-cybersecurity-requirements-as-compliance-as-code/
[15] Van der Stock A (2021) CycloneDX joins OWASP as a flagship project. (OWASP) Available at https://owasp.org/executive/director/2021/06/11/cyclonedx-joins-owasp
[16] The Linux Foundation (2025) About SPDX. Available at https://spdx.dev/about/overview/
[17] National Institute of Standards and Technology (2025) NIST IR 8356. Available at https://doi.org/10.6028/NIST.IR.8356