The OSCAL Futurist

Musings on What is Possible and What is Needed

Greg Elin, Sr. Principal OSCAL Engineer, RegScale Inc.
gelin@regsacle.com
November 30, 2022
Breaking News...

TYSONS CORNER, VA. – November 29, 2022 – RegScale, a next-generation Governance Risk and Compliance (GRC) software company, today announced that it has acquired GovReady, an open-source Compliance-as-Code platform.

GovReady CEO Greg Elin will join RegScale’s R&D team as its OSCAL leader and Compliance-as-Code evangelist along with other members of the GovReady team.
OSCAL is a first step, not a destination

Project Goals

• Decrease Paperwork
  “Drive a large decrease in the paperwork burden”

• Improve System Security Assessments
  “Improve efficiency, timeliness, accuracy, of system security assessments”

• Enable Continuous Assessment
  “Assessed security state more often, ideally continuously”

Design Principles

• Interoperable Data Formats
  “Interoperable, extensible, machine-readable formats”

• Be Relevant Now, Enable a Better Future
  “Ongoing evolution”

Providing control-related information in machine-readable formats.

NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL), a set of formats expressed in XML, JSON, and YAML. These formats include representations of control catalogs, control baselines, and system security assessment results.
1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSLs emerge for compliance content
1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSLs emerge for compliance content
Remember those books explaining DevOps?

Jan 2013

Nov 2019
New book explaining audit compliance in DevSecOps pipeline
New book explains continuous compliance in DevSecOps

- New “Investment Unlimited” book explains rationale and process for continuous compliance in the pipeline

- Rationale can help us create the needed policies for automated continuous ATO to be mandatory
• Add security scans to “build” evidence
• Add cryptographic signatures to “package” evidence for audits
• Add audit evidence packages to “artifact repo”
• Add risk gates to before deployment to assess if evidence indicates sufficient compliance with security
OSCAL’s (temporary) audit evidence challenge

- Using OSCAL to collect evidence requires all OSCAL models
- Few organizations or vendors have implemented all OSCAL models
- DevSecOps can use “scaffold” Assessment Plan and Assessment Results to do Proof of Concepts
It is agency policy to support the acceleration and measurement of the RMF process through approved digital/automated mechanisms and vendor-independent data schemas to programmatically:

(1) Represent System Security Plan (SSP) and SSP-related documents in machine-readable NIST recommended formats;

(2) Generate and update the SSP and related artifacts with changes to the information system to ensure that recent system changes are promptly reflected in such documentation;

(3) Support real-time, on-demand, and publication-subscription sharing of system, threat, vulnerability, POA&M, risk, and risk-decision information among need-to-know parties;

(4) Progressively replace manual and ad-hoc methods of information and data interchange (i.e., spreadsheets, email) with automated processes;

(5) Progressively replace manual and ad-hoc methods of collecting audit-related information with automated processes;

(6) Track duration of activities within the Risk Management Framework (RMF) process to support continuous improvement;

(7) Progressively associate system data in with organization-approved labels and categories to facilitate Zero Trust capabilities and the continuous protection of the confidentiality and use of data across different systems;

(8) Associate system data and assets to specific information systems and assessment boundaries when such data and assets are created to enable the automatic and prompt identification of parties who are responsible that data and asset security; and

(9) Prevent the creation, deployment, or modification of assets not associated with specific information systems and assessment boundaries and permit the Risk Official to approve the quarantine and/or termination of such assets.
1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSL emerge for compliance content
Security tools start speaking OSCAL-ish

OSCAL-ish (In Small Hunks)

- Security tools may need only specific information
- APIs and CLIs designed for certain bits
- How do we exchange small hunks? (APIs/CLI)
- How do we manage small hunks?
Security tools start speaking OSCAL-ish to each other

OSCAL-ish (In Small Hunks)

• Security tools may need only specific information
• APIs and CLIs designed for certain bits
• How do we manage/exchange small hunks?

We need to also talk about...

uuids & props
(durations & signatures)
The OSCAL Futurist predicts

1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSLs emerge for compliance content
The Sensitive System of Record Dilemma … solved with Integrated GRCs

As Imagined...
Sensitive System of Record centralizes information to reduce work for users

In Reality...
Fewer trusted users spend time sharing information to larger numbers of parties without access

Solution... Integrated GRCs
Integrated GRCs extend data management back to multiple business lines to get work done
Solving the Sensitive System of Record Dilemma

As Imagined...
Sensitive System of Record centralizes information to reduce work for users

In Reality...
Fewer trusted users spend time sharing information to larger numbers of parties without access

Solution... Integrated GRCs
Integrated GRCs extend data management back to multiple business lines to get work done

© RegScale, 2022
1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSLs emerge for compliance content
Assessors are Techies, too

Assessors need better tools, not dumbed down tools

• Every info worker has smart phone
• Every info work working uses video, many apps
• ISSOs / Assessors are overwhelmed
• Admins ran data centers – now code does; Admins leveled up to platform engineers
• Assessors deserve better tools
• It’s not them, its our docs (and workshops)
1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSL emerges for compliance content
Community drives adoption

Community

- Workshops
- Examples
- Documentation
- Train the Trainer
- Videos
- Chat & Discord
- Q&A FAQ

>
1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSLs emerge for compliance content
SBOMs will facilitate components

SBOMs, now mandatory, will evolve into carrying OSCAL Component Model data generated by software producers.

1. Consistent with the NIST Guidance and by the timelines identified below, agencies are required to obtain a self-attestation from the software producer before using the software.

2. Agencies may obtain from software producers artifacts that demonstrate conformance to secure software development practices, as needed.
   a. A Software Bill of Materials (SBOM) may be required by the agency in solicitation requirements, based on the criticality of the software as defined in M-21-30, or as determined by the agency. If required, the SBOM shall be retained by the agency, unless the software producer posts it publicly and provides a link to that posting to the agency.
   b. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report “The Minimum Elements for a Software Bill of Materials (SBOM),”1 or successor guidance as published by the Cybersecurity and Infrastructure Security Agency (CISA).
   c. Agencies shall consider reciprocity of SBOM and other artifacts from software producers that are maintained by other Federal agencies, based on direct applicability and currency of the artifacts.

   The Federal Government relies on information and communications technology (ICT) products and services to carry out critical functions. The global supply chain for these technologies faces relentless threats from nation-state and criminal actors seeking to steal sensitive information and intellectual property, compromise the integrity of Government systems, and conduct other acts that impact the United States Government’s ability to safely and reliably provide services to the public.

   Executive Order (EO) 14028, Improving the Nation’s Cybersecurity (May 12, 2021), focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs the National Institute of Standards and Technology (NIST) to issue guidance “identifying practices that enhance the security of the software supply chain.”2 The NIST Secure Software Development Framework (SSDF), SP 800-218,3 and the NIST Software Supply Chain Security Guidance 4 (those two documents, taken together, are hereinafter referred to as “NIST Guidance”) include a set of practices that create the foundation for developing secure software. The EO further directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines. This memorandum requires agencies to comply with the NIST Guidance and any subsequent updates.

---

1 Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
2 Executive Order on Improving the Nation’s Cybersecurity (EO 14028), Section 6(a)
3 Available at: https://csrc.nist.gov/Projects/ssdf
1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSLs emerges for compliance content
How close is OSCAL to a DSL?

“A domain-specific language (DSL) is a computer language specialized to a particular application domain.”

Why OSCAL is not (yet) a DSL

- OSCAL is very entity oriented (e.g., nouns)
- OSCAL only captures state of system (for data exchange)
- OSCAL reflects state but does not change state
Docker-compose is a DSL

Docker-compose

- Specifies services
- Performs actions (verbs!)
- Variable passing
- A “runner” (build process)
Terraform is a DSL

- Specifies resources
- Performs actions (verbs!)
- Variable passing
- A “runner” (build process)
OSCAL – the start of a DSL?

What doAn OSCAL DSL would enhance reuse significantly

- Specifies services
- Performs actions (verbs!)
- Variable passing
- A “runner” (build process)
The OSCAL Futurist predicts

1. Continuous ATO becomes mandatory
2. Security tools start speaking OSCAL-ish
3. Integrated GRCs solve the Sensitive Systems of Records Dilemma
4. Assessors treated as tech-savvy
5. Community drives adoption
6. SBOMs drive component creation and sharing
7. DSLs emerge for compliance content
Which tools will/should speak OSCAL-ish first?

Very good question. Very helpful if scanning tools can understand share some OSCAL hunks to make it easier to consume evidence and understand some scaffolding to catalogs and SSPs to SAP evidence. It would be nice if Active Directory and Authentication tools spoke about parties. SOC tools understanding incoming OSCAL-ish to provide context.

How do we contact you?

- https://community.regscale.com
- gelin@regscale.com
- https://gitter.im/usnistgov-OSCAL (@gregelin)
- Example control set: https://github.com/usnistgov/OSCAL/issues/1383
Thank you!

- https://community.regscale.com
- gelin@regscale.com
- https://gitter.im/usnistgov-OSCAL (@gregelin)