RegScale

RegScale - Continuous Authority to Operate (CATO) Demonstration Using OSCAL with Automated Assessments and Risk Modeling

J. Travis Howerton, Co-Founder and CTO
RegScale
thowerton@regscale.com
https://www.regscale.com

Agenda

1) Speaker Background and Bio
2) OSCAL Support
    1) Free content creation/publishing tools
    2) Export of Catalogs, Profiles, System Security Plans (SSPs), Components, Security Assessment Plans (SAP), and Security Assessment Reports (SAR)
3) Overview of ATARC Pilot and End to End OSCAL Demonstration
4) Integration with FedRAMP Threat-Based Risk Model using OSCAL
5) RegScale CLI for OSCAL processing

Speaker Background and Bio

- Started as a Federal employee at Y-12 Nuclear Weapons Plant
- Became NNSA's first Chief Technology Officer (CTO)
- Former Deputy CIO at Oak Ridge National Lab (ORNL)
- Bechtel lead for merger of Y-12 and Pantex nuclear manufacturing
- Currently RegScale Co-Founder and Chief Technology Officer
- Masters Degree in Computer Information Systems from Boston University
- CISSP, PMP, ITIL, Scrum Master, Harvard Credential of Readiness

OSCAL Publishing Tools

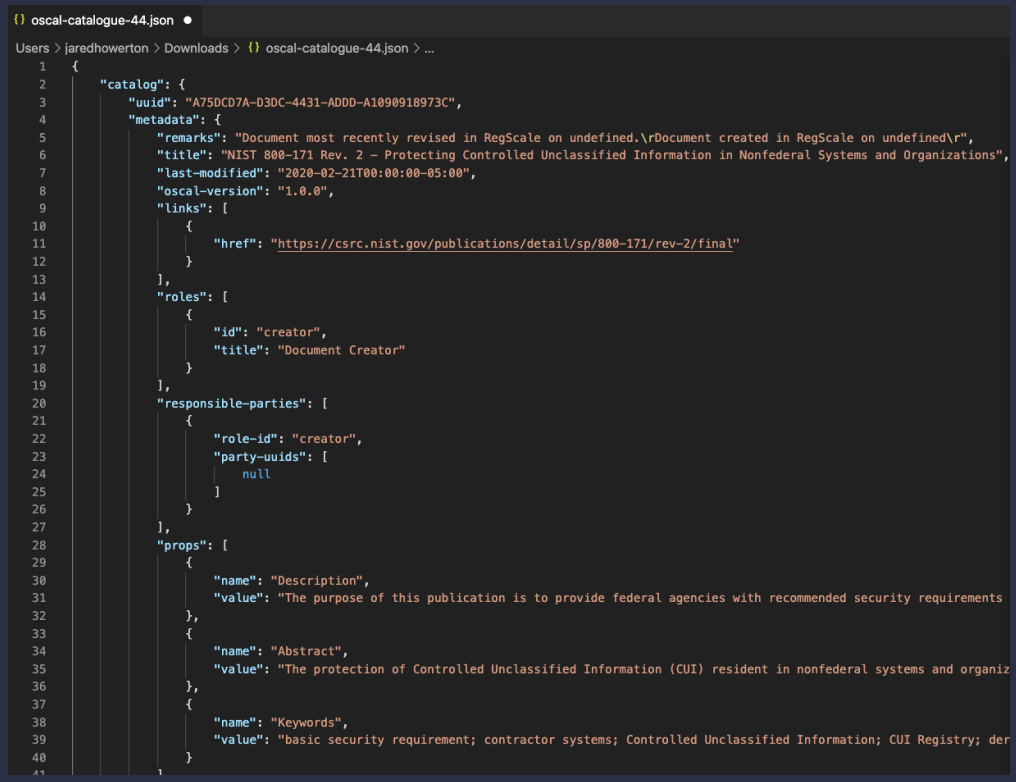
- In our opinion, one of the main barriers to OSCAL adoption is the lack of tools for generating and publishing OSCAL content
- While NIST provides catalogs and profiles for 800-53, there are many commercial standards and agency-specific overlays that are also required to fully implement OSCAL in most organizations
- Most security professional do not have the time, skills, or inclination to re-create their catalogs in JSON/XML
- In addition, we assume most are unwilling or unable to pay extra to do so

We believe that a key enabler for OSCAL will be robust and free tooling for creating and publishing OSCAL content.

RegScale Community Edition (CE)

- Completely free to download and install
- Supports the full OSCAL stack
- Create content by hand, copy and paste, or leverage APIs to script
- Any compliance requirement can be converted to OSCAL – not just cyber security

Get Started - https://regscale.com/get-started



NIST 800-171 Rev. 2 OSCAL

NIST 800-171 Rev. 2 Example

Steps to Produce the OSCAL:

- Downloaded an Excel spreadsheet with 800-171 controls and converted to JSON
- Mapped fields to RegScale Catalog/Control schema in Python
- Leveraged APIs to create and bulk upload controls
- Logged into RegScale and click “Export OSCAL” button to get the OSCAL JSON file
- Total Effort: < 2 hours

OSCAL Layers Supported:

Catalog (Import/Export)
Profile (Import/Export)
System Security Plan (Import/Export)
Component (Export)
Assessment Plan (Export)
Assessment Results (Export)
Plan of Action and Milestones (Export)

Supports OSCAL Version 1.0.0

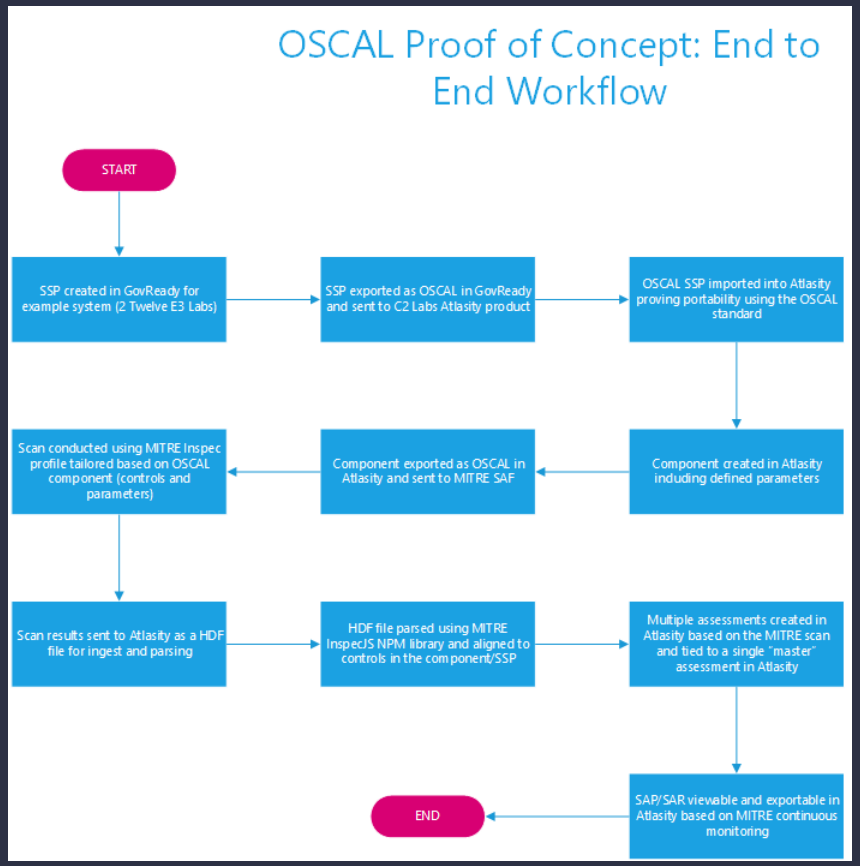
Other Examples

While we gave a specific example, we have OSCAL versions of all RegScale catalogs (now up to 73), examples include:

1) Cloud Security Alliance Cloud Controls Matrix (CCM)
2) Air Force Management Instruction 63-1201
3) GDPR and California Consumer Privacy Act (CCPA)
4) Center for Internet Security (CIS) Controls Version 8
5) Cybersecurity Maturity Model Certification (CMMC)
6) DHS 4300A Handbook
7) Defense Security Servive (DSS) – Electronic Communication Plan (ECP)

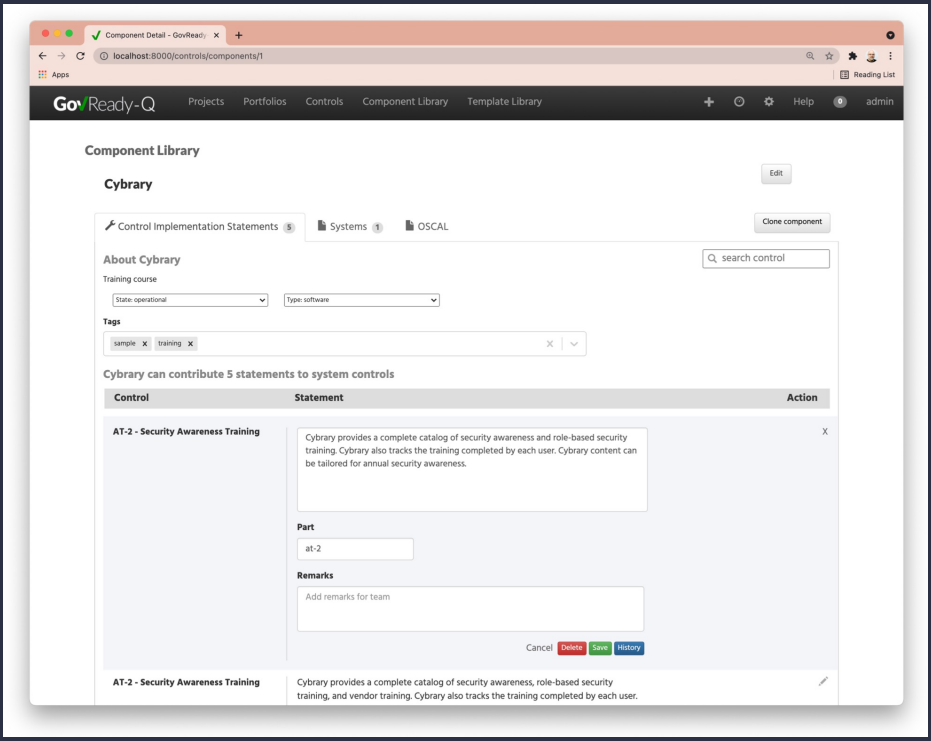
All RegScale catalogs can be converted and exported to OSCAL.

ATARC Pilot



- End-to-End Proof of Concept (research paper pending)
- Demonstrates interoperability between GovReady, RegScale, and MITRE using OSCAL
- Exercised the full stack and provided valuable feedback on lessons learned and challenges
- Example stack for doing a continuous ATO in a cloud environment for a subset of controls

ATARC Pilot – Step 1



- SSP created in GovReady and exported as OSCAL (prior RC version)
- OSCAL ingested into RegScale using our APIs
- Multiple tweaks to our schema and UI made to accommodate the 1.0 standard
- Data enriched in the GUI to prep for future steps
- Component created with specific parameters

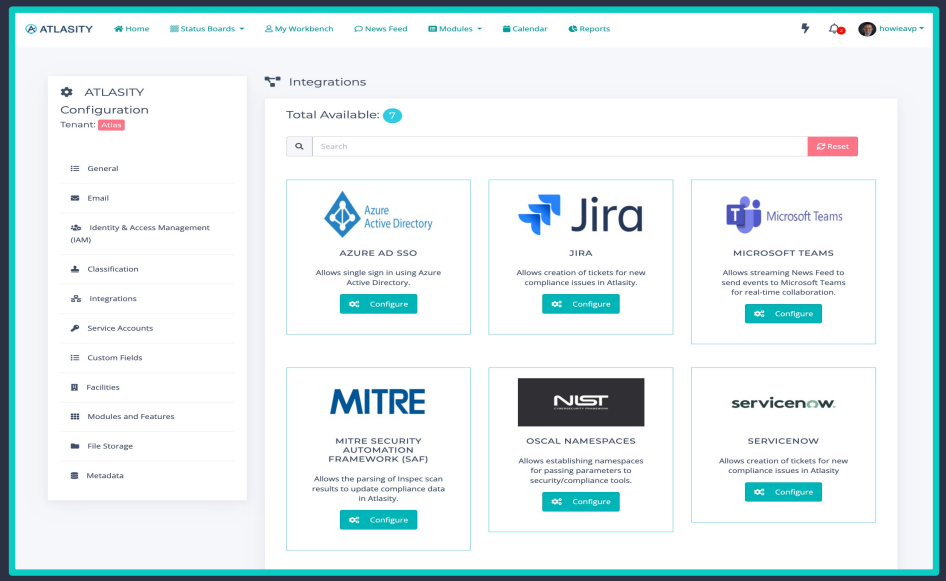
ATARC Pilot – Step 2

RegScale

- RegScale sends component OSCAL file to MITRE SAF
- Custom Inspec profile generated based on parameters and a scan was run against the environment
  - Used an extension model to strongly type parameters
- Scan results exported as a HDF file
- HDF file imported and parsed into RegScale

ATARC Pilot – Step 3

RegScale

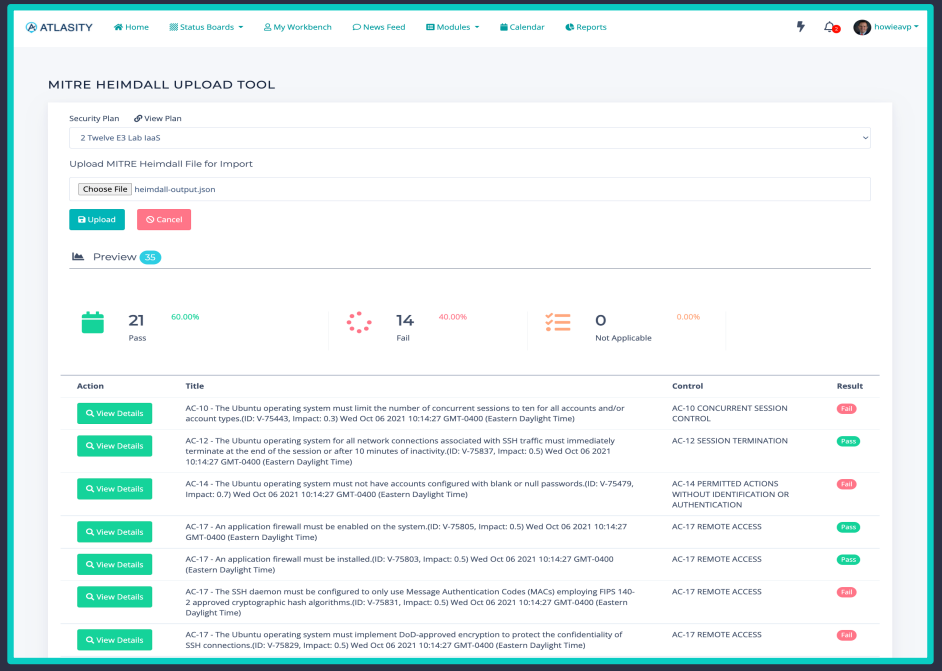


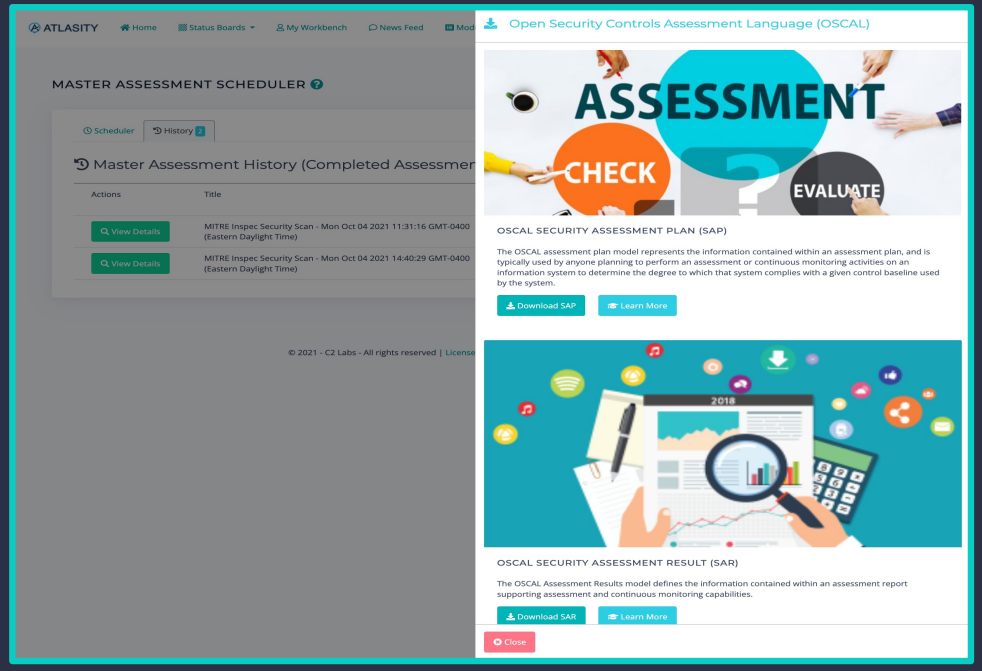
- HDF file mapped to Control IDs sent via OSCAL and sharded out as many control assessments in RegScale
- RegScale data plus the Inspec Profile data used to generate the SAP
- HDF results data from the scan used to generate the SAR

Roundtrip from GovReady -> RegScale -> MITRE SAF -> RegScale completed using OSCAL

ATARC Pilot – Final Results

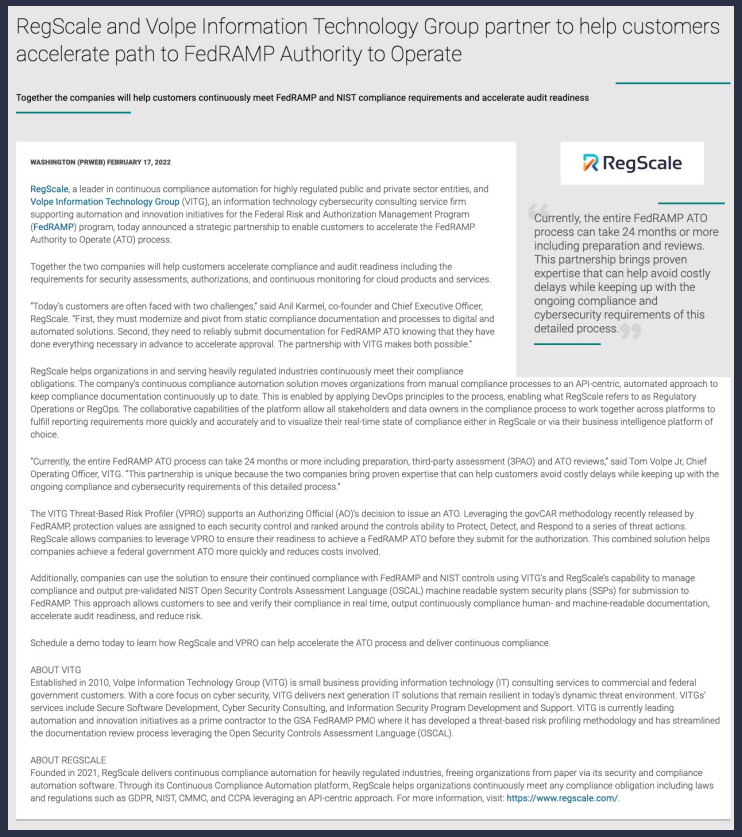
RegScale





Threat-Based Risk Modeling

- Customers have expressed a desire to focus on the controls that have the most impact on risk based on current threats
- RegScale partnered with VITG to integrate the FedRAMP threat-based risk model based on govCAR
- Data exchange 100%-based on OSCAL
- Goals – reduced costs to obtain a FedRAMP approval plus increased focus on risk reduction and risk tolerances



RegScale and Volpe Information Technology Group partner to help customers accelerate path to FedRAMP Authority to Operate

Together the companies will help customers continuously meet FedRAMP and NIST compliance requirements and accelerate audit readiness

WASHINGTON (PRWEB) FEBRUARY 17, 2022

RegScale, a leader in continuous compliance automation for highly regulated public and private sector entities, and Volpe Information Technology Group (VITG), an information technology cybersecurity consulting service firm supporting automation and innovation initiatives for the Federal Risk and Authorization Management Program (FedRAMP) program, today announced a strategic partnership to enable customers to accelerate the FedRAMP Authority to Operate (ATO) process.

Together the two companies will help customers accelerate compliance and audit readiness including the requirements for security assessments, authorizations, and continuous monitoring for cloud products and services.

"Today's customers are often faced with two challenges," said Anil Karmel, co-founder and Chief Executive Officer, RegScale. "First, they must modernize and pivot from static compliance documentation and processes to digital and automated solutions. Second, they need to reliably submit documentation for FedRAMP ATO knowing that they have done everything necessary in advance to accelerate approval. The partnership with VITG makes both possible."

RegScale

"Currently, the entire FedRAMP ATO process can take 24 months or more including preparation and reviews. This partnership brings proven expertise that can help avoid costly delays while keeping up with the ongoing compliance and cybersecurity requirements of this detailed process."

RegScale helps organizations in and serving heavily regulated industries continuously meet their compliance obligations. The company's continuous compliance automation solution moves organizations from manual compliance processes to an API-centric, automated approach to keep compliance documentation continuously up to date. This is enabled by applying DevOps principles to the process, enabling what RegScale refers to as Regulatory Operations or RegOps. The collaborative capabilities of the platform allow all stakeholders and data owners in the compliance process to work together across platforms to fulfill reporting requirements more quickly and accurately and to visualize their real-time state of compliance either in RegScale or via their business intelligence platform of choice.

"Currently, the entire FedRAMP ATO process can take 24 months or more including preparation, third-party assessment (3PAO) and ATO reviews," said Tom Volpe Jr, Chief Operating Officer, VITG. "This partnership is unique because the two companies bring proven expertise that can help customers avoid costly delays while keeping up with the ongoing compliance and cybersecurity requirements of this detailed process."

The VITG Threat-Based Risk Profiler (VPRO) supports an Authorizing Official (AO)'s decision to issue an ATO. Leveraging the govCAR methodology recently released by FedRAMP, protection values are assigned to each security control and ranked around the controls ability to Protect, Detect, and Respond to a series of threat actions. RegScale allows companies to leverage VPRO to ensure their readiness to achieve a FedRAMP ATO before they submit for the authorization. This combined solution helps companies achieve a federal government ATO more quickly and reduces costs involved.

Additionally, companies can use the solution to ensure their continued compliance with FedRAMP and NIST controls using VITG's and RegScale's capability to manage compliance and output pre-validated NIST Open Security Controls Assessment Language (OSCAL) machine readable system security plans (SSPs) for submission to FedRAMP. This approach allows customers to see and verify their compliance in real time, output continuously compliance human- and machine-readable documentation, accelerate audit readiness, and reduce risk.

Schedule a demo today to learn how RegScale and VPRO can help accelerate the ATO process and deliver continuous compliance.

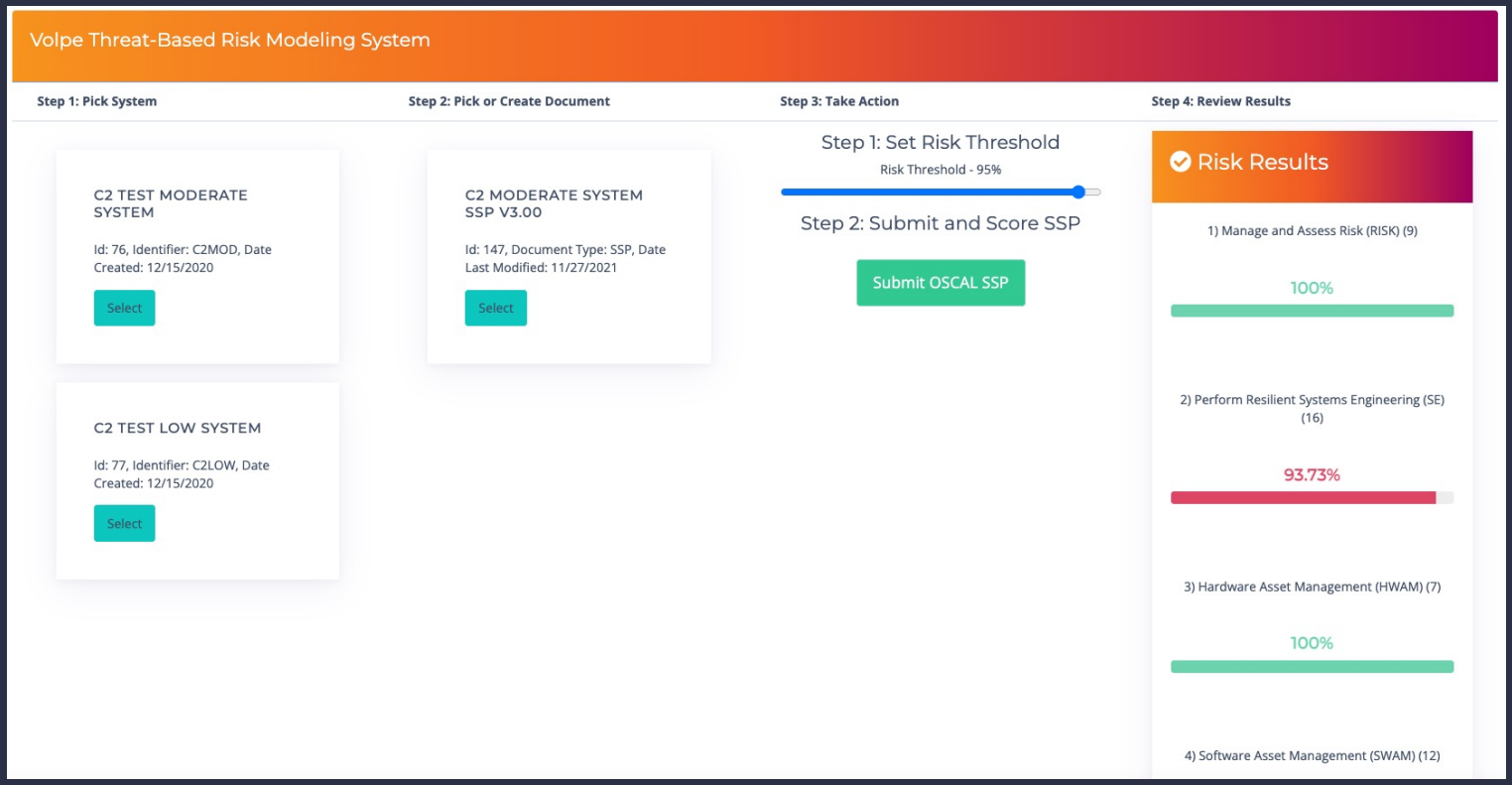
ABOUT VITG

Established in 2010, Volpe Information Technology Group (VITG) is small business providing information technology (IT) consulting services to commercial and federal government customers. With a core focus on cyber security, VITG delivers next generation IT solutions that remain resilient in today's dynamic threat environment. VITGs' services include Secure Software Development, Cyber Security Consulting, and Information Security Program Development and Support. VITG is currently leading automation and innovation initiatives as a prime contractor to the GSA FedRAMP PMO where it has developed a threat-based risk profiling methodology and has streamlined the documentation review process leveraging the Open Security Controls Assessment Language (OSCAL).

ABOUT REGSCALE

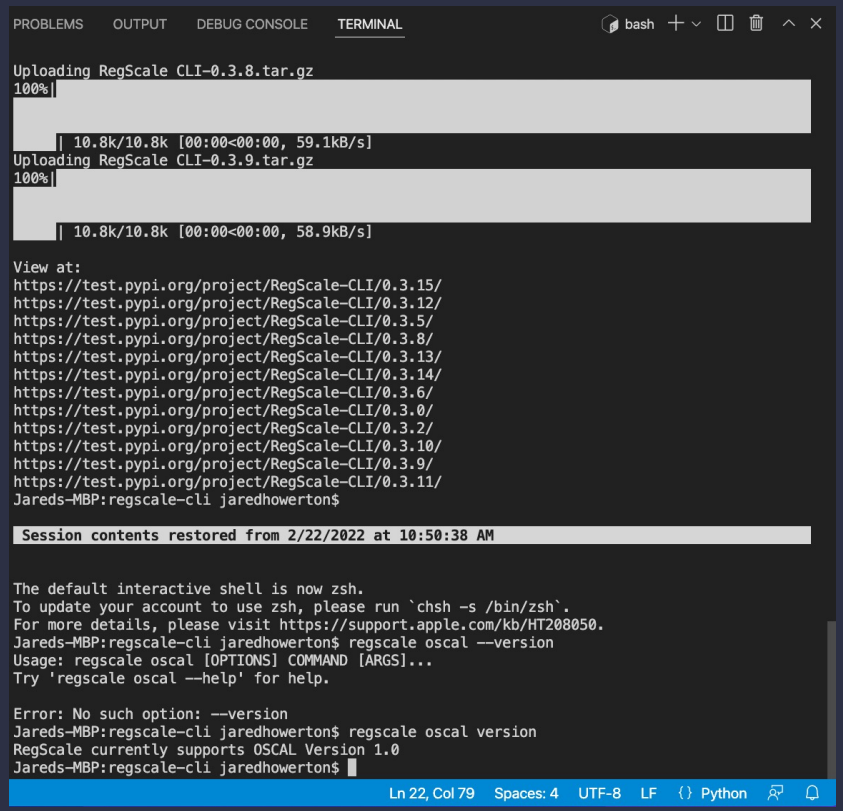
Founded in 2021, RegScale delivers continuous compliance automation for heavily regulated industries, freeing organizations from paper via its security and compliance automation software. Through its Continuous Compliance Automation platform, RegScale helps organizations continuously meet any compliance obligation including laws and regulations such as GDPR, NIST, CMMC, and CCPA leveraging an API-centric approach. For more information, visit: https://www.regscale.com/.

Risk Modeling Results – VITG -> RegScale



OSCAL CLI (BETA)

- All of our previous work was done using custom Python scripts against our APIs or GUI-driven features in the platform
- We wanted to make it easier to work with and integrate OSCAL at scale so we built a Python Command Line Interface (CLI) – now in private customer BETA
- Allows bulk processing and loading of OSCAL data via jobs or could run in a container for scheduled Kubernetes jobs



Questions?

thowerton@regscale.com

Learn More

https://www.regscale.com