RegScale – Extreme Automation with OSCAL- Exercising the Full OSCAL Stack in a Next Generation GRC

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

Agenda

- **Speaker Background and Bio**
- **OSCAL Support**
  - Free content creation/publishing tools (NOTE: not open source)
  - Export of Catalogs, Profiles, System Security Plans (SSPs), Components, Security Assessment Plans (SAP), and Security Assessment Reports (SAR)
  - All OSCAL support is included in our free Community Edition (CE)
- **Dynamic OSCAL Content Authoring**
- **Integration with FedRAMP Threat-Based Risk Model using OSCAL**
- **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

RegScale

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 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.

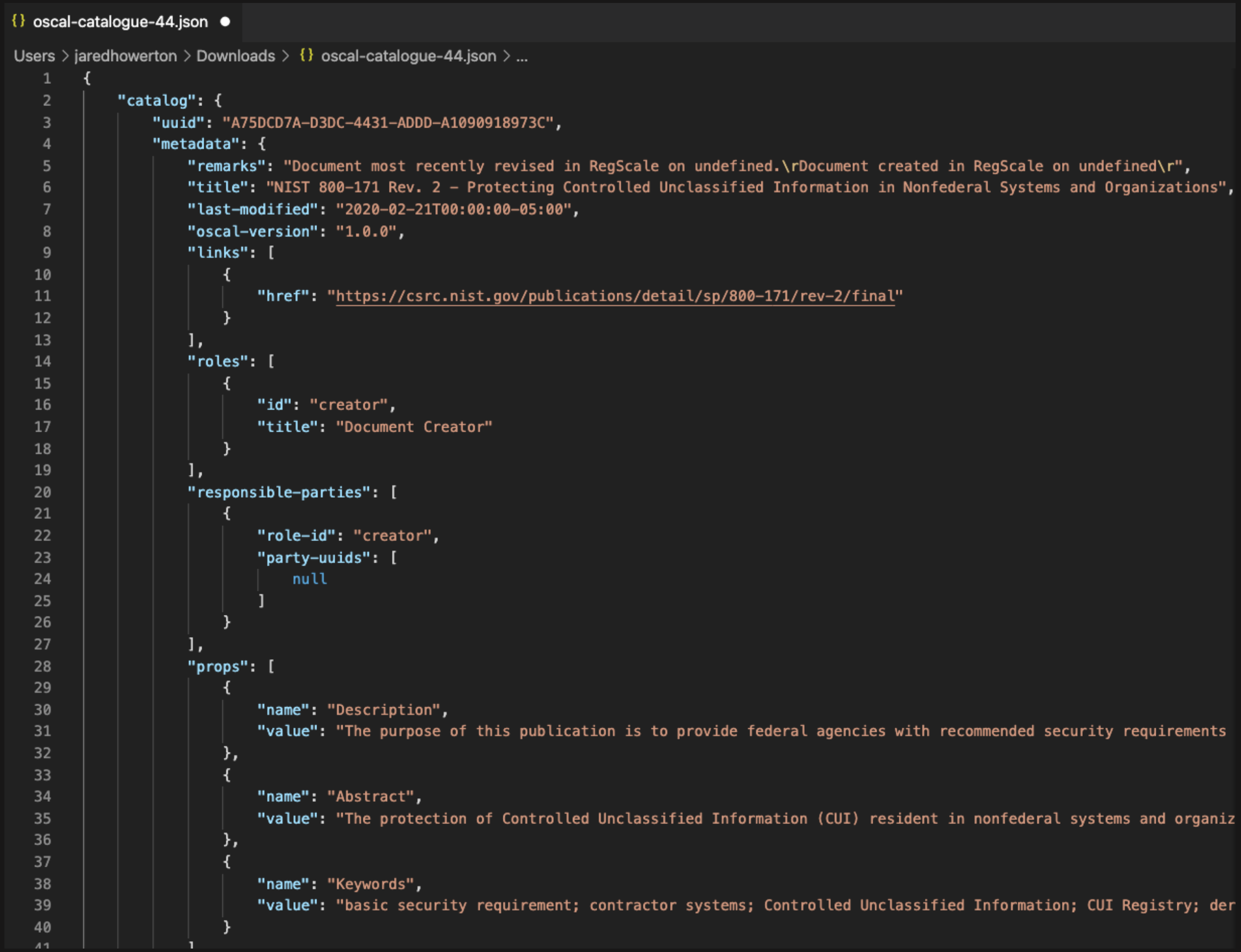
RegScale Community Edition CE

RegScale

The RegScale Solution

- 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


oscal-catalogue-44.json
Users > jaredhowerton > Downloads > oscal-catalogue-44.json > ...

```json
{
    "catalog": {
        "uuid": "A75DCD7A-D3DC-4431-ADDD-A1090918973C",
        "metadata": {
            "remarks": "Document most recently revised in RegScale on undefined.\rDocument created in RegScale on undefined\r",
            "title": "NIST 800-171 Rev. 2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations",
            "last-modified": "2020-02-21T00:00:00-05:00",
            "oscal-version": "1.0.0",
            "links": [
                {
                    "href": "https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final"
                }
            ],
            "roles": [
                {
                    "id": "creator",
                    "title": "Document Creator"
                }
            ],
            "responsible-parties": [
                {
                    "role-id": "creator",
                    "party-uuids": [
                        null
                    ]
                }
            ],
            "props": [
                {
                    "name": "Description",
                    "value": "The purpose of this publication is to provide federal agencies with recommended security requirements
                },
                {
                    "name": "Abstract",
                    "value": "The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organiz
                },
                {
                    "name": "Keywords",
                    "value": "basic security requirement; contractor systems; Controlled Unclassified Information; CUI Registry; der
                }
            ]
```

NIST 800-171 Rev. 2 OSCAL

New Features Since NIST Last Talk

RegScale

- **Digitized 20+ new catalogues**
- **Added support for sub-control level-data:**
    - Objectives
    - Parameters
    - Options (pre-loaded list of available options)
    - Test Plan (i.e. 800-53A)
    - CCI Support (alignment to STIGs)

Demo

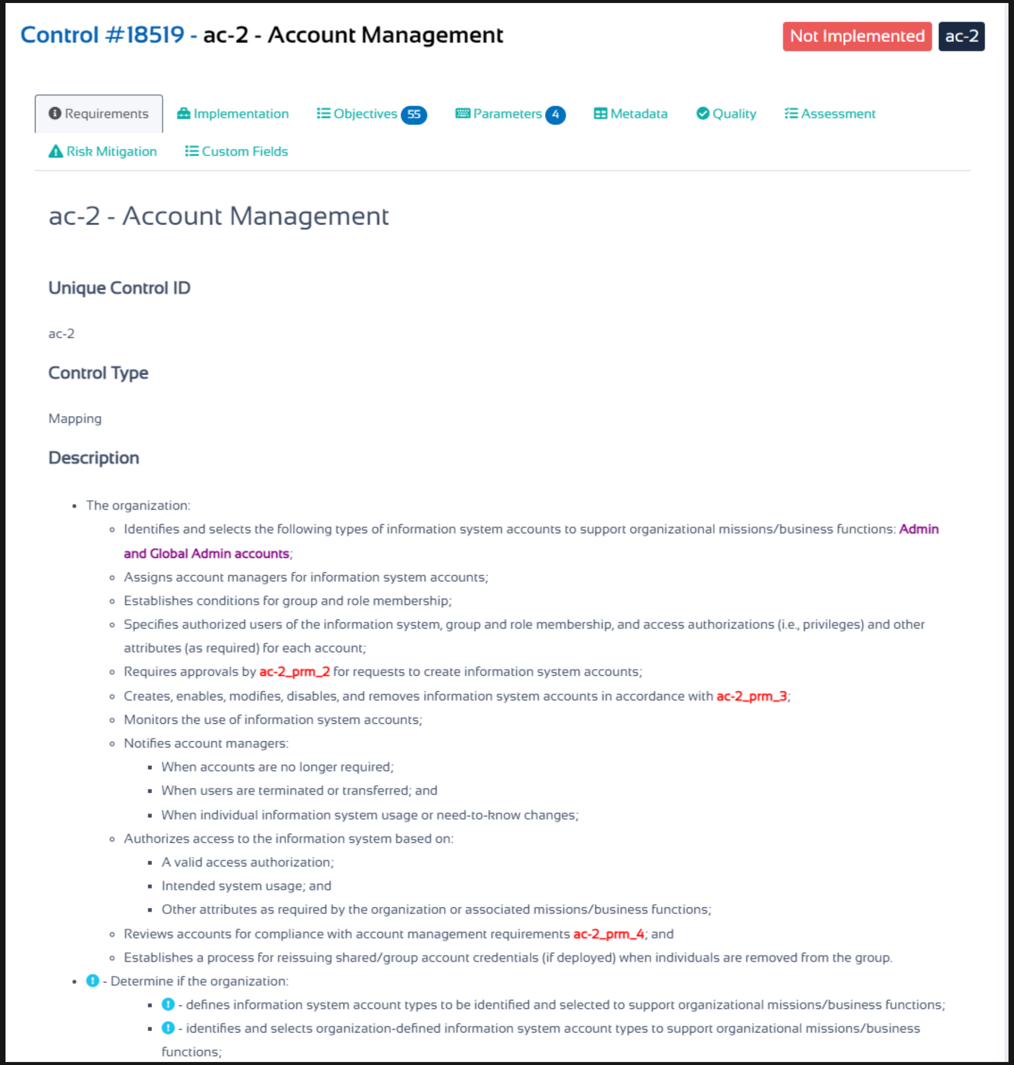
- Review catalogs available - RegScale – Regulations
- View 800-53 Catalogs in RegScale
  - RegScale - Catalogues
- Export Non-NIST Catalog to OSCAL (CRI Profile Tier 4)
  - RegScale - Catalogues

Demo (continued)

- Converting a catalog from Excel to RegScale/OSCAL
- Script/source code - internal-scripts/ig-3-importer.py at main · RegScale/internal-scripts (github.com)
- Result in RegScale - RegScale - Catalogues

Dynamic OSCAL Content Authoring

RegScale



Control #18519 - ac-2 - Account Management

ac-2 - Account Management

Unique Control ID

ac-2

Control Type

Mapping

Description

- The organization:
  - Identifies and selects the following types of information system accounts to support organizational missions/business functions: **Admin and Global Admin accounts**;
  - Assigns account managers for information system accounts;
  - Establishes conditions for group and role membership;
  - Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
  - Requires approvals by **ac-2_prm_2** for requests to create information system accounts;
  - Creates, enables, modifies, disables, and removes information system accounts in accordance with **ac-2_prm_3**;
  - Monitors the use of information system accounts;
  - Notifies account managers:
    - When accounts are no longer required;
    - When users are terminated or transferred; and
    - When individual information system usage or need-to-know changes;
  - Authorizes access to the information system based on:
    - A valid access authorization;
    - Intended system usage; and
    - Other attributes as required by the organization or associated missions/business functions;
  - Reviews accounts for compliance with account management requirements **ac-2_prm_4**; and
  - Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
- ! - Determine if the organization:
    - ! - defines information system account types to be identified and selected to support organizational missions/business functions;
    - ! - identifies and selects organization-defined information system account types to support organizational missions/business functions;

1. Load controls in the GUI along with their objectives and parameters
2. Update the objective status via the GUI
3. Update parameter settings via the GUI
4. Watch the policy update in real-time

Demo

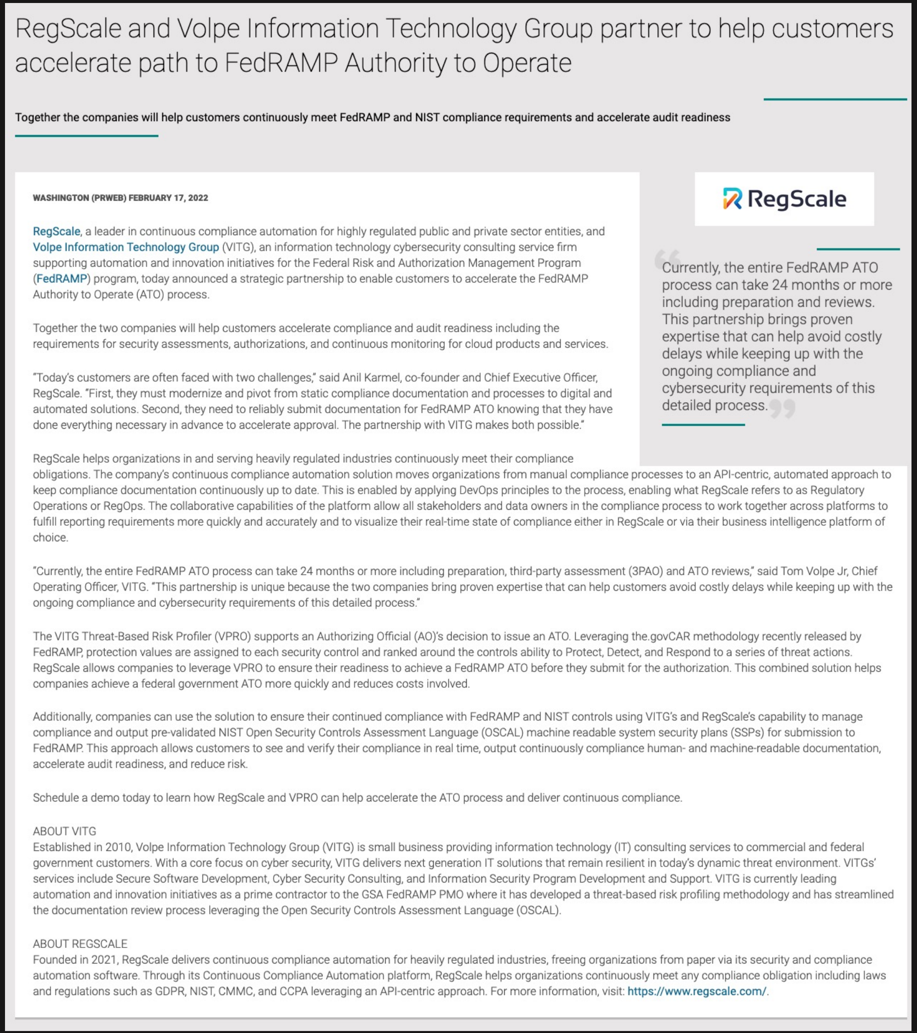
- Assess Control Objectives - RegScale - Control Implementations
- Update Parameters
- View dynamic updates to the policy/requirements
- Load Assessments from default (800-53A)
- Conduct a Lightning Assessment
- View an Automated Assessment via API/CLI - RegScale - Issues

Upcoming Work

- eMASS and FedRAMP Export of POAMs (Excel)
- Adding more scanners (Tenable, Qualys, etc.)
- Adding more ITIL tools (Salesforce Service Cloud)

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

> 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.

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 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.

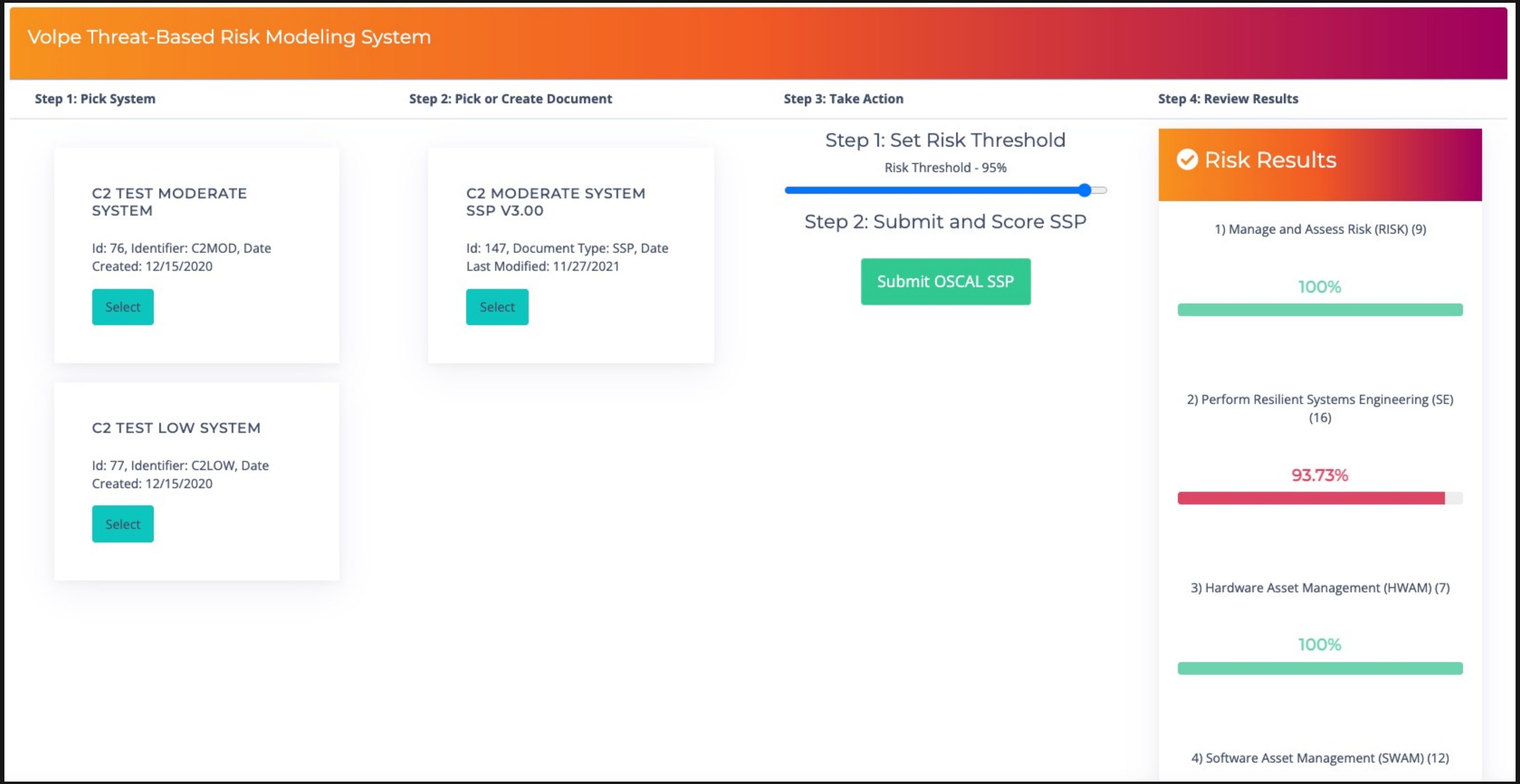
Schedule a demo today to learn how RegScale and VPRO can help accelerate the ATO process and deliver continuous compliance.

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**

RegScale



Volpe Threat-Based Risk Modeling System

Step 1: Pick System

C2 TEST MODERATE SYSTEM

Id: 76, Identifier: C2MOD, Date Created: 12/15/2020

Select

C2 TEST LOW SYSTEM

Id: 77, Identifier: C2LOW, Date Created: 12/15/2020

Select

Step 2: Pick or Create Document

C2 MODERATE SYSTEM SSP V3.00

Id: 147, Document Type: SSP, Date Last Modified: 11/27/2021

Select

Step 3: Take Action

Step 1: Set Risk Threshold

Risk Threshold - 95%

Step 2: Submit and Score SSP

Submit OSCAL SSP

Step 4: Review Results

Risk Results

1) Manage and Assess Risk (RISK) (9)

100%

2) Perform Resilient Systems Engineering (SE) (16)

93.73%

3) Hardware Asset Management (HWAM) (7)

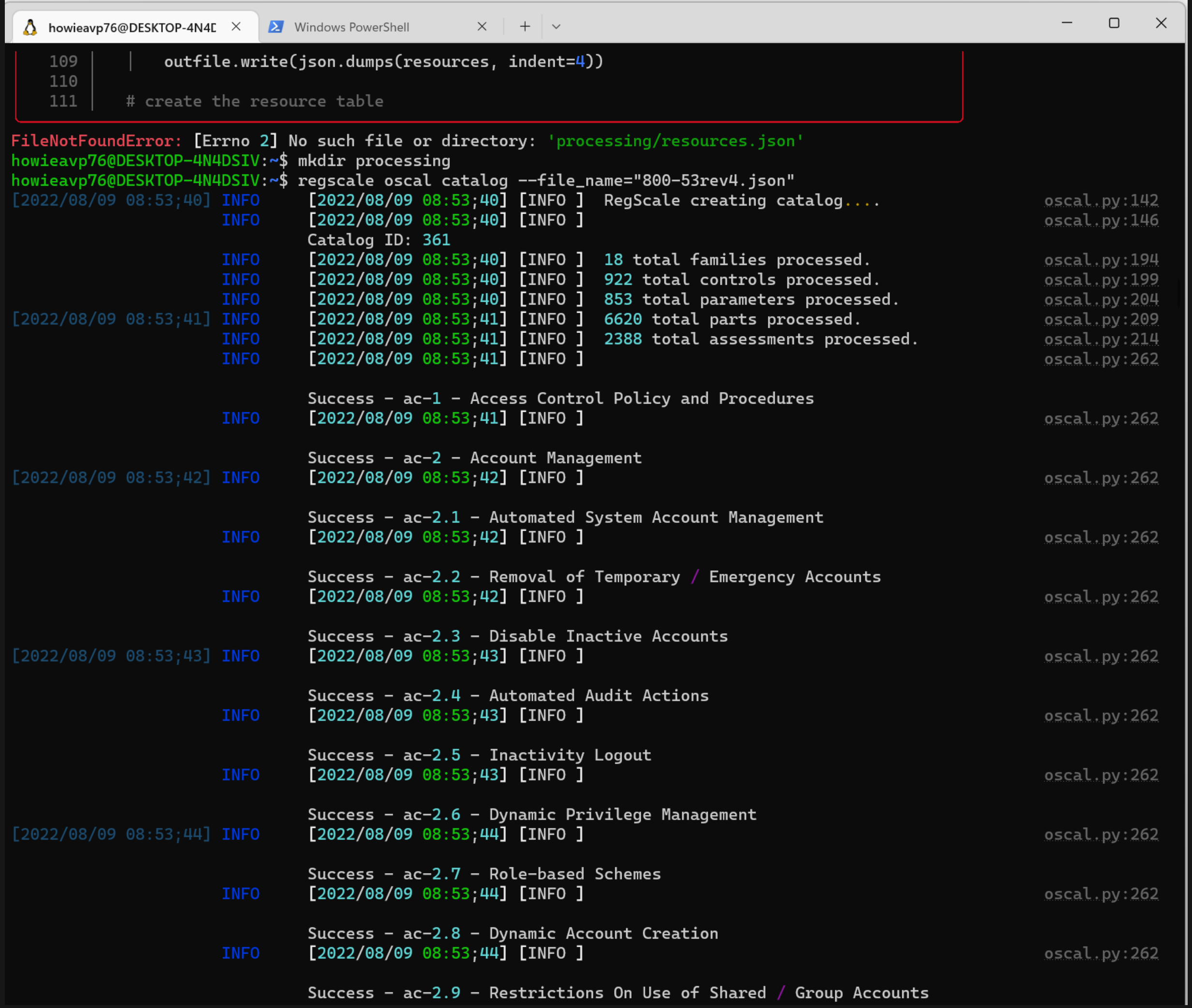
100%

4) Software Asset Management (SWAM) (12)

OSCAL CLI

RegScale

- 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) – RegScale-CLI · PyPI
- Documentation – RegScale
- Allows bulk processing and loading of OSCAL data via jobs or could run in a container for scheduled Kubernetes jobs - Docker Hub



```
    │   outfile.write(json.dumps(resources, indent=4))

  # create the resource table
FileNotFoundError: [Errno 2] No such file or directory: 'processing/resources.json'
howieavp76@DESKTOP-4N4DSIV:~$ mkdir processing
howieavp76@DESKTOP-4N4DSIV:~$ regscale oscal catalog --file_name="800-53rev4.json"
[2022/08/09 08:53;40] INFO     [2022/08/09 08:53;40] [INFO ]  RegScale creating catalog....              oscal.py:142
                      INFO     [2022/08/09 08:53;40] [INFO ]                                             oscal.py:146
                               Catalog ID: 361
                      INFO     [2022/08/09 08:53;40] [INFO ]  18 total families processed.               oscal.py:194
                      INFO     [2022/08/09 08:53;40] [INFO ]  922 total controls processed.              oscal.py:199
                      INFO     [2022/08/09 08:53;40] [INFO ]  853 total parameters processed.            oscal.py:204
[2022/08/09 08:53;41] INFO     [2022/08/09 08:53;41] [INFO ]  6620 total parts processed.                oscal.py:209
                      INFO     [2022/08/09 08:53;41] [INFO ]  2388 total assessments processed.          oscal.py:214
                      INFO     [2022/08/09 08:53;41] [INFO ]                                             oscal.py:262

                               Success - ac-1 - Access Control Policy and Procedures
                      INFO     [2022/08/09 08:53;41] [INFO ]                                             oscal.py:262

                               Success - ac-2 - Account Management
[2022/08/09 08:53;42] INFO     [2022/08/09 08:53;42] [INFO ]                                             oscal.py:262

                               Success - ac-2.1 - Automated System Account Management
                      INFO     [2022/08/09 08:53;42] [INFO ]                                             oscal.py:262

                               Success - ac-2.2 - Removal of Temporary / Emergency Accounts
                      INFO     [2022/08/09 08:53;42] [INFO ]                                             oscal.py:262

                               Success - ac-2.3 - Disable Inactive Accounts
[2022/08/09 08:53;43] INFO     [2022/08/09 08:53;43] [INFO ]                                             oscal.py:262

                               Success - ac-2.4 - Automated Audit Actions
                      INFO     [2022/08/09 08:53;43] [INFO ]                                             oscal.py:262

                               Success - ac-2.5 - Inactivity Logout
                      INFO     [2022/08/09 08:53;43] [INFO ]                                             oscal.py:262

                               Success - ac-2.6 - Dynamic Privilege Management
[2022/08/09 08:53;44] INFO     [2022/08/09 08:53;44] [INFO ]                                             oscal.py:262

                               Success - ac-2.7 - Role-based Schemes
                      INFO     [2022/08/09 08:53;44] [INFO ]                                             oscal.py:262

                               Success - ac-2.8 - Dynamic Account Creation
                      INFO     [2022/08/09 08:53;44] [INFO ]                                             oscal.py:262

                               Success - ac-2.9 - Restrictions On Use of Shared / Group Accounts
```

Demo

RegScale

- Load a NIST 800-53 catalog via the CLI
  - regscale oscal catalog --file_name="800-53rev4.json"
- Create a profile from an uploaded catalog
  - regscale oscal profile –title="NIST Mini Workshop" –categorization="Low" –catalog=61 –file_name="low-profile.json"
- Export the new catalog in RegScale JSON
- Export the new catalog in RegScale OSCAL

Demo (continued) – Work in Progress

- Take the JSON OSCAL and convert to YAML
- Take the JSON OSCAL and convert to XML
- Example commands below:
- Docker (run container) - docker run -v /C/Users/howie/cli:/data -it regscale/regscale-cli:latest ash
- Convert SSP -> XML - regscale oscal convert-catalog-json-xml "oscal-ssp-example.json" "oscal-ssp.xml"
- Convert SSP -> YAML - regscale oscal convert-json-yaml "oscal-ssp-example.json" "oscal-ssp.yaml"

Contributors

- Juliette Easley, Full Stack Developer, [(2) Juliette Easley | LinkedIn]
- Bryan Eaton, Data Engineer, [(2) Bryan Eaton | LinkedIn]

Follow Up

Questions?

thowerton@regscale.com

Learn More

Website: https://www.regscale.com

RegScale Blog - Introducing Dynamic OSCAL Content Authoring

CLI Docs: https://regscale.com/documentation/cli-oscal

CLI on PyPi: https://pypi.org/project/RegScale-CLI/

CLI Container:
https://hub.docker.com/repository/docker/regscale/regscale-cli