OSCAL tools and integration and interoperability
NIST 2nd OSCAL Workshop, Feb 2021
GovReady Open Source GRC

Making Compliance Easier

User Focus → User Friendly
Step-by-step guidance regardless of compliance expertise

API for Continuous Monitoring
Dynamically push CI/CD scans, ports & protocols, and more into SSP

Pre-Assessment
Give Devs and ISSO’s a way to secure themselves early in the SDLC

Secure Platform
- Supports database encryption
- Supports FIPS 140-2 certified systems
- HTTPS TLS encrypted sessions
- Single Sign On (Proxy Authentication)
- Granular Access Control
GovReady started with the idea that compliance is not security and you shouldn’t have to read hundreds of pages to get an ATO. We developed for the compliance-as-code revolution that is now arriving.

**Federal Funded R&D, Pilots**

DHS S&T Research & Development contract and pilot funding

R&D Funding
- DHS S&T funds R&D
- User Centered Research
- Early prototypes

Pilot funding
- DHS S&T funds Pilots
- DHS Digital service funds prototyping
- B&D Consulting (for Navy) Pilot
- DOD Contractor uses for 800-171
- Fortune 50 Healthcare Co testing

Early Adopters
- DHS CBP Pilot > Adoption Decision
- Fortune 50 Healthcare Co adopts for internal cyber assessments
- Accepted into DCode Accelerator
- RMF 2.0 Data Automation SME support for USDA CISO

Enterprise Deployments
- Deployment in DHS CBP Cloud
- GovReady ATO (in progress)
- Air Force SBIR Awardee (800-171)
- Commercial IT Managed Services (PCI)
- Wazuh Endpoint monitoring integration
GovReady’s Special Focus on Steps 1-3 of the RMF

**Friendly ATO Information, Tutorials**

Provide your System teams with a platform for learning—and sharing tips—on succeeding with their controls and ATO before they start.

**Support Legacy GRC Workflow**

Enterprise locked into a legacy GRC workflow? GovReady's designed to send structured data to your existing tool.

**Collaborative Control Authoring**

GovReady's modern control authoring tools are easier to use and more productive than spreadsheets. Our collaborative environment supports writing machine-readable standardized implementations mapped to system components for easier reuse.

---

1. **Categorize**
2. **Select**
3. **Implement**
4. **Assess**
5. **Authorize**
6. **Monitor**

---

- **0. Learn**
  - Provide your System teams with a platform for learning—and sharing tips—on succeeding with their controls and ATO before they start.
GovReady is built around next generation, machine-readable compliance content format NIST OSCAL.

**OSCAL Control Catalogue**
GovReady controls catalogs use NIST OSCAL format under the hood.

**Support for Compliance as Code**
GovReady control content editing is designed to map control content to system elements and produce machine-readable OSCAL component information.

**Compliance as Code Pioneer**
GovReady has been involved with Compliance as Code initiatives from the beginning.
Flexible, complimentary support for ATP and ATO processes

Description

DHS CBP Office of Information & Technology (OIT) picked GovReady to pilot for Lightweight ATO over legacy GRC tools because of its easier customization. Pilot proved GovReady supported standardized control narratives, online PTA process, and generating Test Plans. Pilot assessed deploying GovReady in CBP’s cloud environment with CBP’s DevOps tools. Decision made for GovReady production deployment to improve the current ATP and ATO process, identifying ways to normalize template language used by common control providers (CCPs), and minimize the burden on the end users, and streamline first three steps of NIST RMF to support other GRC tools.

Surprise Value in Privacy Threshold Analysis

Pilot revealed new utility and use cases for DHS Privacy Offices and the Privacy Threshold Analysis (PTA).

Decision to Move Forward to Production

Pilot concluding with decision to move GovReady into full production within CBP.

Deployed in CBP Cloud Environment

GovReady-Q deployed in a DHS cloud environment with support for DHS SSO and CBP DevOps Pipeline.
Download SSP OSCAL JSON

...and we're done

Available documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSP v1</td>
<td>Word (docx)</td>
</tr>
<tr>
<td>SSP v1 (OSCAL/JSON)</td>
<td>OSCAL (json)</td>
</tr>
<tr>
<td>SSP v1 (OSCAL/XML)</td>
<td>OSCAL (xml)</td>
</tr>
</tbody>
</table>

Your Answers

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>No questions needed to be answered in this section.</td>
<td></td>
</tr>
</tbody>
</table>

Continue to ATO Letter

Return to project

Review

![Code snippet showing a system security plan in JSON format](sspv1_oscal_json.json)
Component Library

Available Components

Test Cmpt Name modified
Test Cmpt2 New Name
Cmpt3 (New Name) And create a description for Cmpt3
Cmpt4
Cmpt5
Cmpt6
Cmpt8
Cmpt10
2 Twelve (Flat)
HelpRace
Auth0
AWS IAM
AWS IAMs - Deprecated test description
Item 1
Component Control Authoring

Test IT System > Selected Controls

AC-3 Access Enforcement

NIST SP-800-53 rev4

Component Implementations Statements

AWS IAM
Status: Implemented
In this architecture, AWS identify and Access Management (IAM) and Amazon S3 enforce access to the AWS infrastructure and data in Amazon S3 buckets. The baseline IAM groups and roles are associated with access policies to align user accounts with personnel functions related to infrastructure/platform management (e.g., Billing, Amazon EC2/VPC/Amazon RDS systems administration, I.T. auditing, etc.) Login/API access is restricted to those users for whom the organization has authorized and created, or federated, IAM user accounts, and assigned the appropriate IAM group and/or role memberships. Amazon S3 buckets have specific access control policies assigned to restrict access to those IAM users who are assigned the appropriate IAM roles/groups.

Active Directory
Status: Planned
b. how we use active directory

Add existing component
Name of component

Add component statement

Open #component_controls on this page in a new tab
DEMO
Demo of Making an SSP
Deployed Features to accelerate RMF Steps 1 - 3

Next Gen Collaborative Questionnaires
- TurboTax-style guided questions
- Imputed questions/answers
- Discuss answers (with attachments)
- Assign questions to users
- 17 question types (datagrid, attachments)
- Dynamic question text (full HTML)
- Portable, YAML-based questionnaires
- In-line review/approve workflow feature
- Dynamic drop-in sub-questionnaires
- Questionnaire authoring tool
- Sample content for “Plan” documents

Output Templates
- Library of artifact templates
- Add custom artifact templates
- Auto-populated SSP
- Auto-populated content links back to questions for easy editing
- Multiple Templates per questionnaire
- Downloadable as Word, Markdown, Text

Simple, RESTful API
- Integrate content from scans
- Populate evidence from systems
- Exchange info with other GRC, tools

Export to spreadsheets
- Generate export data for legacy GRC

Enterprise-Ready
- Single Sign On
- Role-based access control
- Container Deployment

Customizable User Interface
- Completely customizable UI to support organization look and feel
- Customize / Replace pages
- Aria-compatible components for 508 accessibility compliance

Compliance-as-Code Control Statement Editor
- Write narratives by component to standardize & reuse content
- View/edit by control or component
- Inherited Common Controls
- Generate OSCAL, OpenControl machine-readable control statements

Project Management
- Portfolios for projects
Lifecycle dashboard displays each project’s progress through the steps of the NIST RMF.

01 Stages of NIST RMF
Lifecycle dashboard displays each project’s progress through the steps of the NIST RMF.

02 Security Control Status
Control implementation now tracked directly in database instead of questionnaires enabling richer metadata management including control status.

03 Next Tasks
Project display redesigned for better linear representation of modules and to dynamically show and hide modules to make next tasks clearer.
Support Templates, Guides

The GovReady application serves to streamline the Authority to Operate (ATO) process by providing a secure environment where teams can collaborate and complete authorization packages across an organization. Team members using GovReady have access to a suite of templates and questionnaires that serve to meet the requirements associated with achieving an ATO quickly.