

GovReady®

Making Compliance Easier
gregelin@govready.com

**OSCAL tools and integration
and interoperability**
NIST 2nd OSCAL Workshop, Feb 2021

GovReady Open Source GRC

Making Compliance Easier

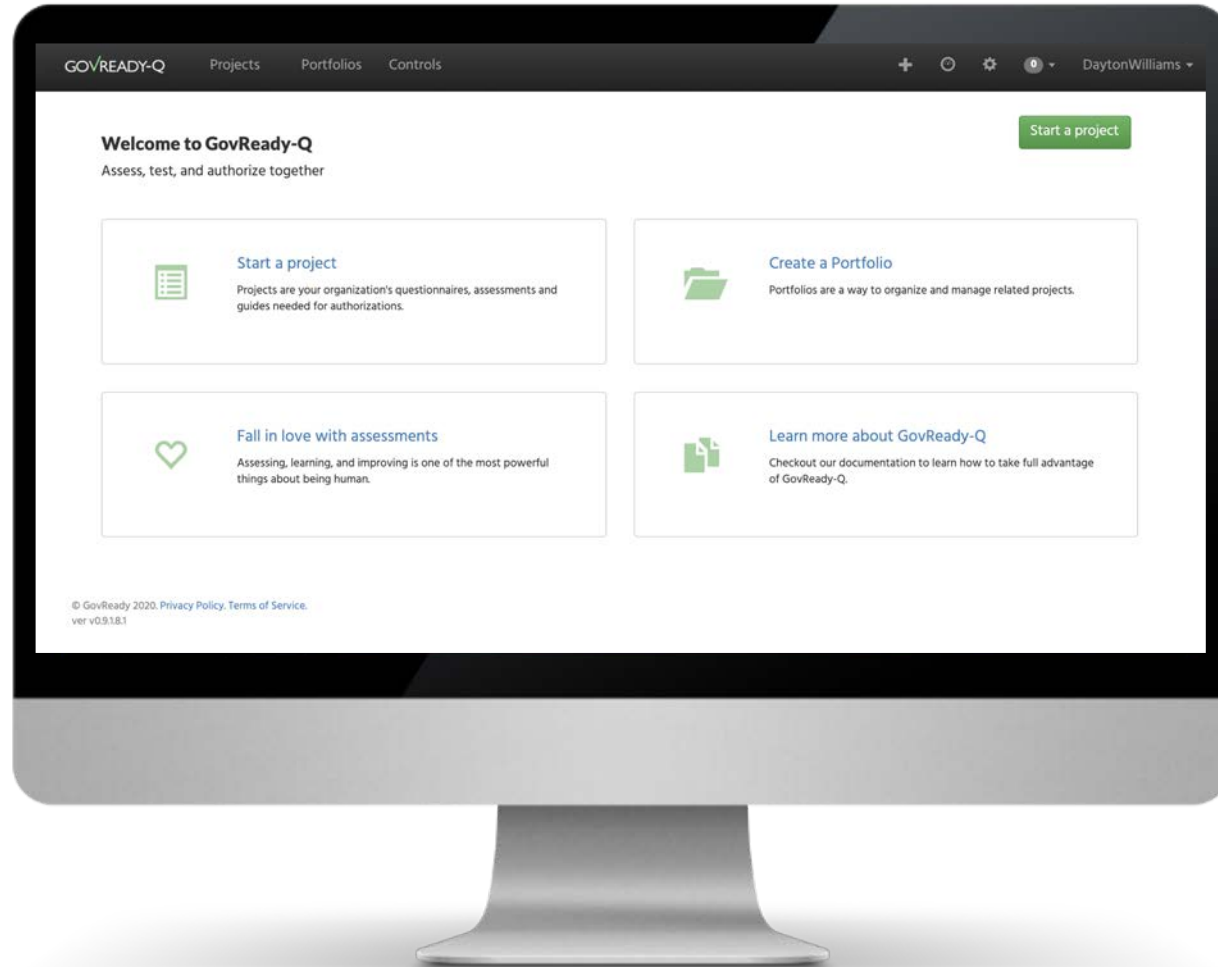
User Focus → User Friendly

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

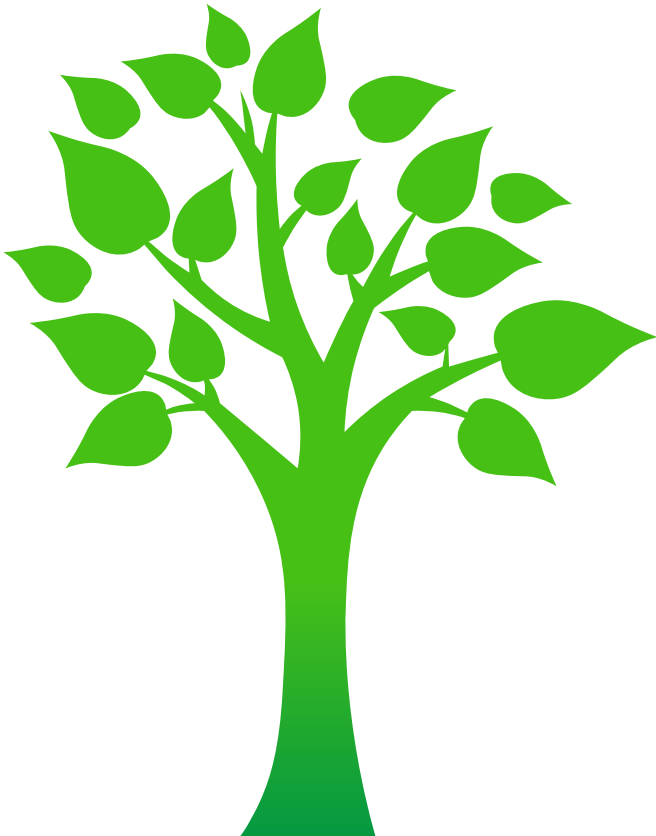
- Supports database encryption
- Supports FIPS 140-2 certified systems
- HTTPS TLS encrypted sessions
- Single Sign On (Proxy Authentication)
- Granular Access Control



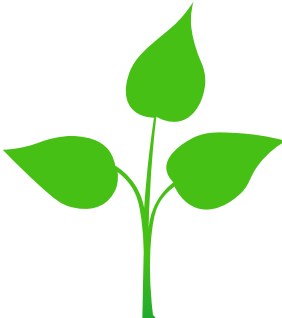
Federal Funded R&D, Pilots

DHS S&T Research & Development contract and pilot funding

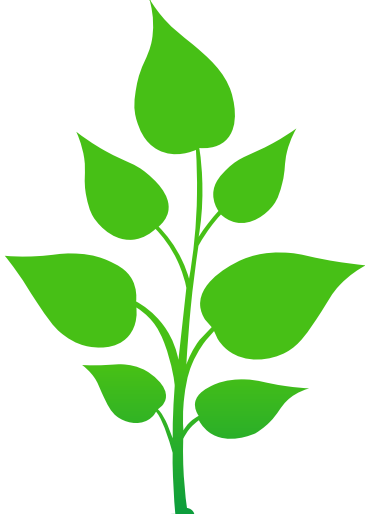
GovReady started with the idea that compliance is not security and you shouldn't have to read hundreds of pages to get an ATO. We developed for the compliance-as-code revolution that is now arriving.



2016



2018



2019

2020

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

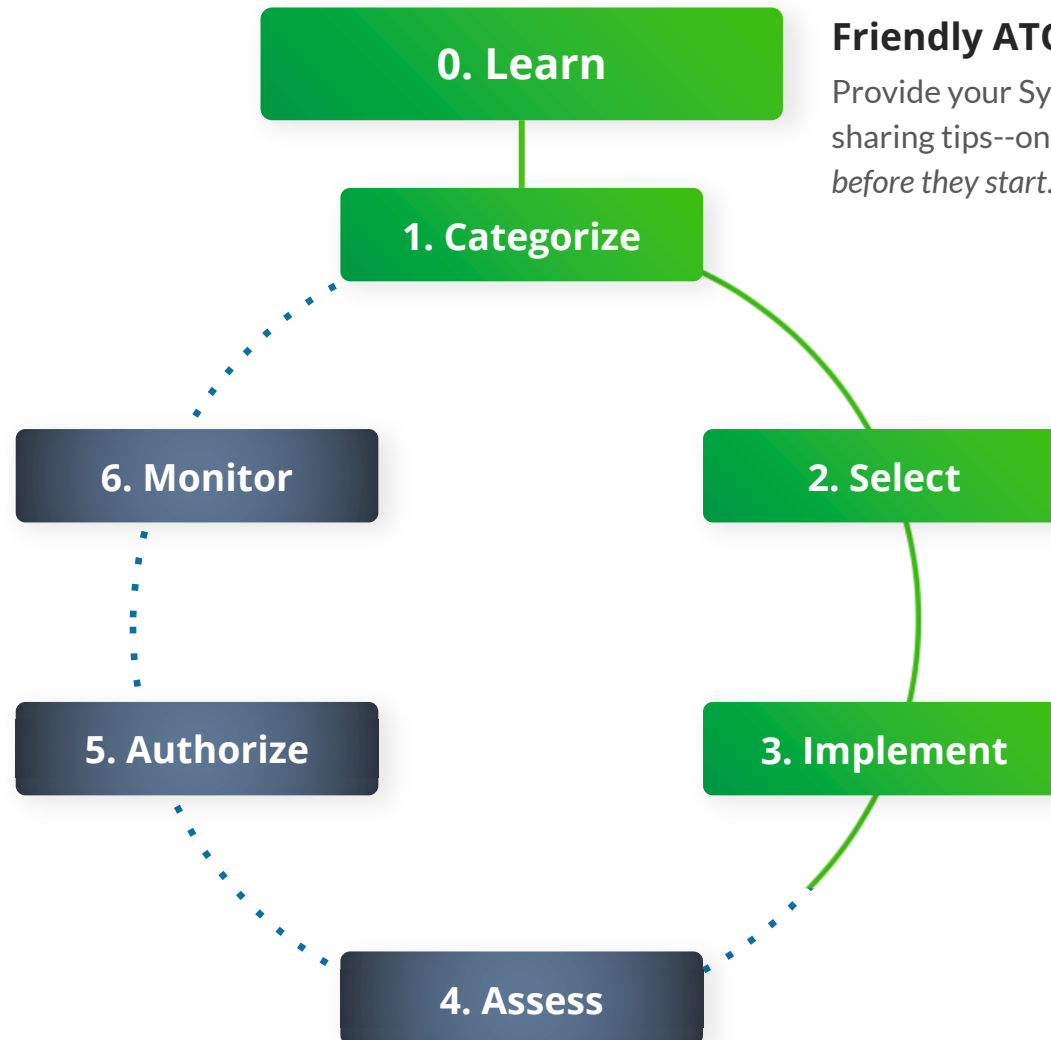
Early Adopters

- 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.

OSCAL-Support Compliance as Code

GovReady is built around next generation, machine-readable compliance content format NIST OSCAL.

OSCAL Control Catalogue

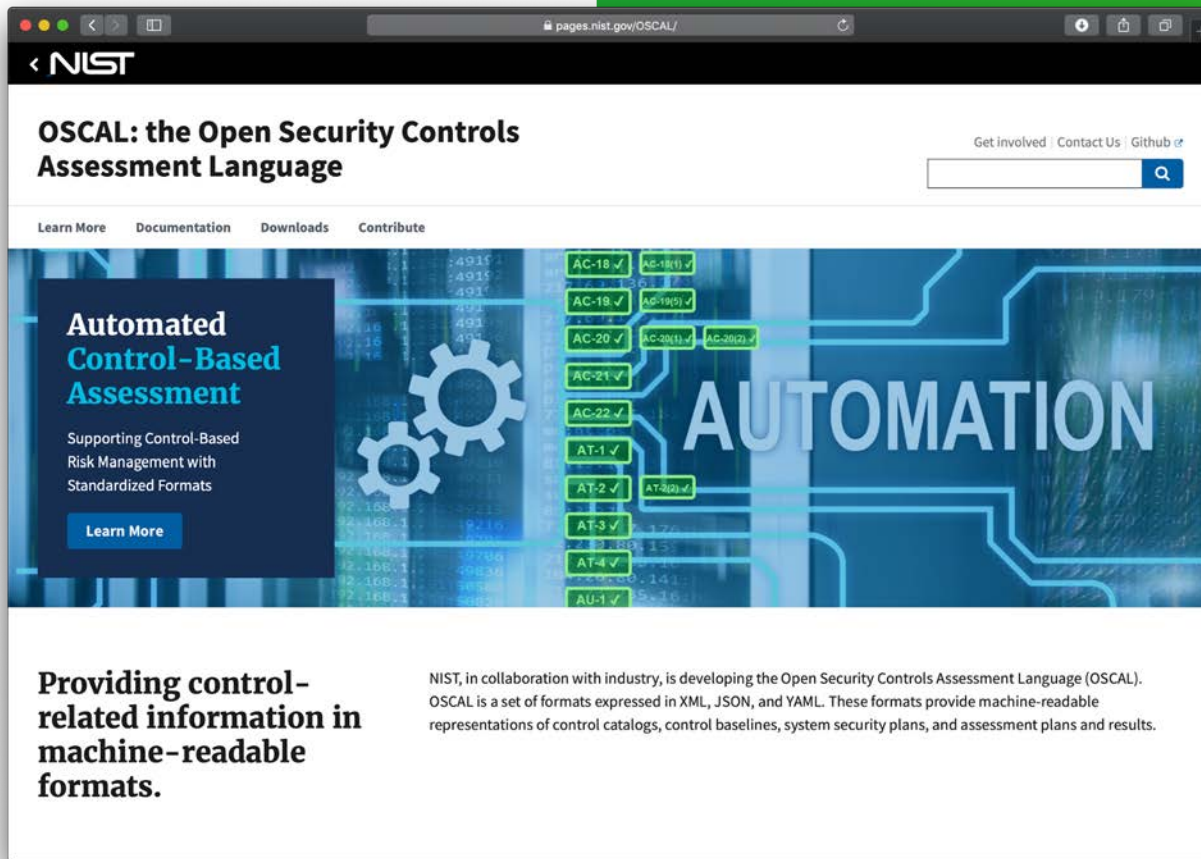
GovReady controls catalogs use NIST OSCAL format under the hood.

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.



The screenshot shows the NIST OSCAL website. The header includes the NIST logo and navigation links: 'Learn More', 'Documentation', 'Downloads', and 'Contribute'. The main content area features a large banner with the word 'AUTOMATION' in the center, surrounded by a grid of control IDs (AC-18, AC-19, AC-20, AC-21, AC-22, AT-1, AT-2, AT-3, AT-4, AU-1) and a gear icon. Below the banner, there is a section titled 'Automated Control-Based Assessment' with a 'Learn More' button. At the bottom, there is a section titled 'Providing control-related information in machine-readable formats.' with a paragraph of text.

Automated Control-Based Assessment
Supporting Control-Based Risk Management with Standardized Formats
[Learn More](#)

Providing control-related information in machine-readable formats.

NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.

DHS CBP

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.

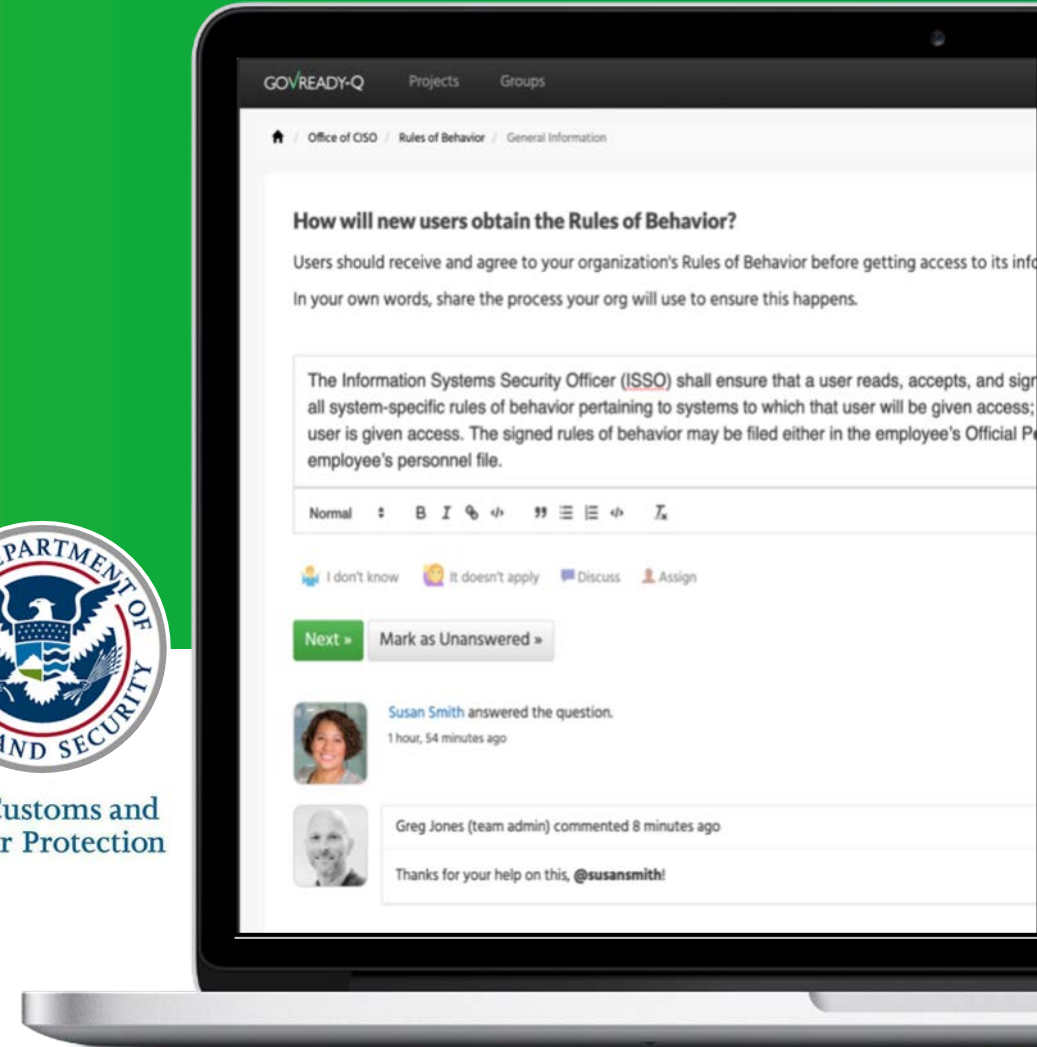


Deployed in CBP Cloud Environment

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



U.S. Customs and Border Protection



Download SSP OSCAL JSON

The image shows a web browser window on the left and a code editor on the right. The browser window displays a page titled "GOVREADY-Q" with a navigation menu and a breadcrumb trail: "CustomerX / Test IT System / System Security Plan". The main content area shows a table of "Available documents" with columns for "Document" and "Downloads". The table lists three documents: "SSP v1", "SSP v1 (OSCAL/JSON)", and "SSP v1 (OSCAL/XML)". Below the table, there is a section for "Your Answers" with a "Question" and "Answer" column, and a message stating "No questions needed to be answered in this section." At the bottom of the page, there are three buttons: "Continue to ATO Letter »", "Return to project", and "Review »".

The code editor on the right shows the content of the "ssp_v1_oscal_json.json" file. The JSON content is as follows:

```
1 {
2   "system-security-plan": {
3     "uuid": "70ec9ef7-8816-4ec2-90b9-57647d761f02",
4     "metadata": {
5       "title": "CustomerX Website",
6       "last-modified": "2021-01-15 15:09:43.025293+00:00",
7       "version": "None",
8       "oscal-version": "1.0.0rc1"
9     },
10    "import-profile": {
11      "href": "profile_path"
12    },
13    "system-characteristics": {
14      "system-ids": [
15        {
16          "id": "govready-75"
17        }
18      ],
19      "system-name": "CustomerX Website",
20      "system-name-short": "CXW",
21      "description": "This system supports CustomerX Website\\.",
22      "security-sensitivity-level": "<FISMA Level>",
23      "system-information": {
24        "information-types": [
25          {
26            "title": "UNKNOWN information type title",
27            "description": "information type description",
28            "confidentiality-impact": {
29              "base": "information type confidentiality impact"
30            },
31            "integrity-impact": {
32              "base": "information type integrity impact"
33            },
34            "availability-impact": {
35              "base": "information type availability impact"
36            }
37          }
38        ]
39      },
40      "security-impact-level": {
41        "security-objective-confidentiality": "UNKNOWN",
42        "security-objective-integrity": "UNKNOWN",
43        "security-objective-availability": "UNKNOWN"
44      },
45      "status": {
46        "state": "operational"
47      },
48      "authorization-boundary": {
49        "description": "System authorization boundary, TBD"
50      }
51    },
52    "system-implementation": {
53      "users": {},
54      "components": {
55        "5255-02e-004b-4095-0030-0131313140"
56      }
57    }
58  }
59 }
```

Component Library

Component Library

You have access to 54 components.

[Manage Import Records](#) [Create a Component](#) [Import OSCAL Component](#)

Available Components	
Test Cmpt Name modified	
Test Cmpt2 New Name	
Cmpt3 (New Name)	And create a description for CMPT3
Cmpt4	
Component1	
Cmpt5	
Cmpt6	
Cmpt8	
Cmpt10	
2 Twelve (Flat)	
HelpRace	
Auth0	
AWS IAM	
AWS IAMs - Deprecated	test description
Item 1	

Component Control **Authoring**

The screenshot shows a web browser window with the URL `localhost:8000/controls/75/controls/catalogs/NIST_SP-800-53_rev4/cont`. The browser's address bar and tabs are visible at the top. The application header includes the logo 'GOVREADY-Q' and navigation links for 'Projects', 'Portfolios', 'Controls', 'Component Library', and 'App Library'. A user profile 'Greg' is shown in the top right corner.

The main content area is titled 'Test IT System > Selected Controls'. On the right side, there is a search input field containing 'AC-3' and a green 'Look up' button. Below this, the section is titled 'AC-3 Access Enforcement' and 'NIST SP-800-53 rev4'. A navigation bar contains tabs for 'Control', 'Component Statements' (with a '2' indicator), 'Combined Statement', 'OSCAL', and 'OpenControl'. The 'Component Statements' tab is active.

Under the 'Component Implementations Statements' heading, there are two entries:

- 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

At the bottom, there is a form to 'Add existing component' with a text input field 'Name of component' and a green 'Submit for related' button. Below the input field is a dropdown menu with the selected option 'Test Cmp Name modified'. A green 'Add component statement' button is located below the dropdown.

A footer note at the bottom left reads: '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

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

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

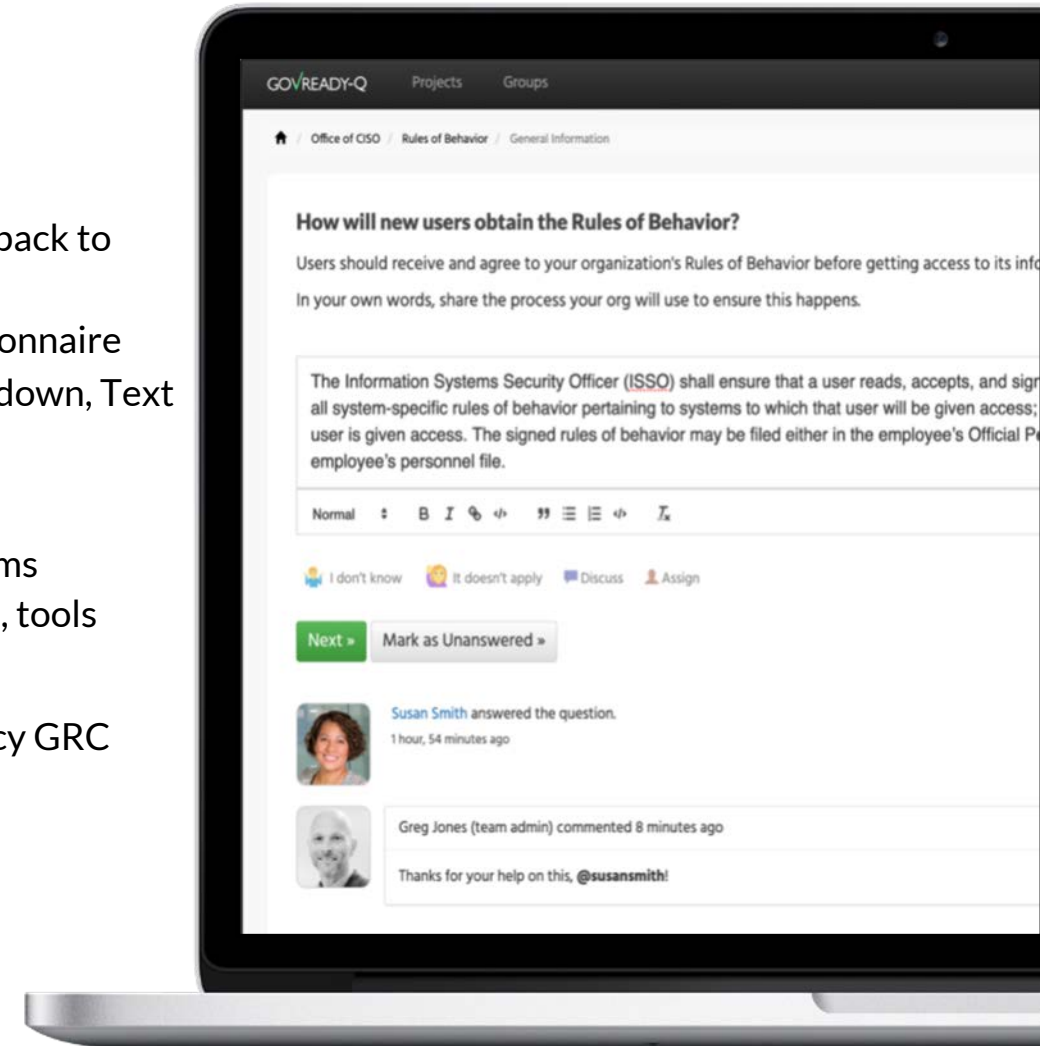
- Generate export data for legacy GRC

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



THANK YOU

www.govready.com

Contact us for additional information on
this contract and GovReady Services.



917-304-3488



gregelin@govready.com

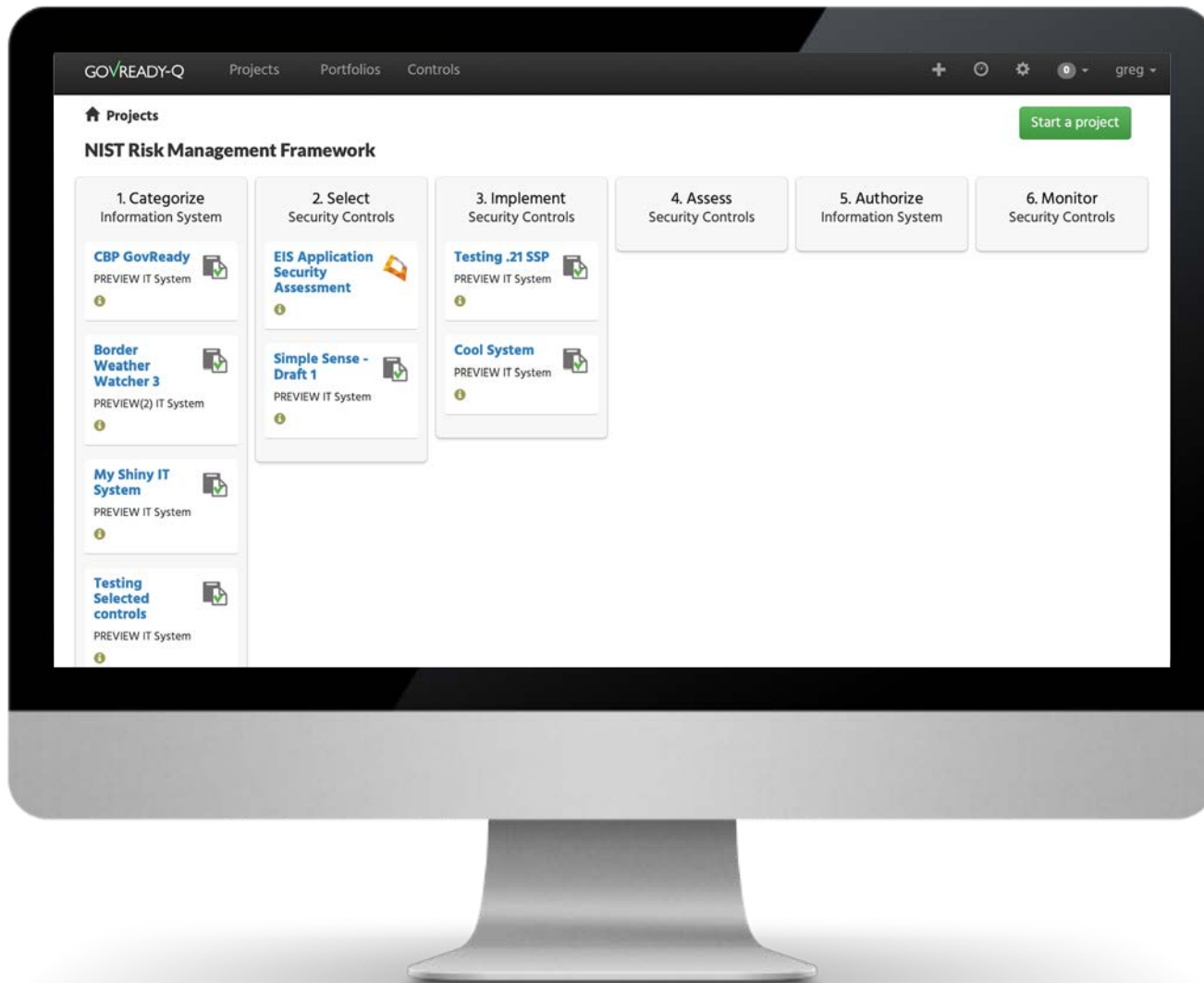


www.govready.com

EXTRA SLIDES

Understanding the RMF

Modern UI for Agile Processes



01

Stages of NIST RMF

Lifecycle dashboard displays each project's progress through the steps of the NIST RMF.

02

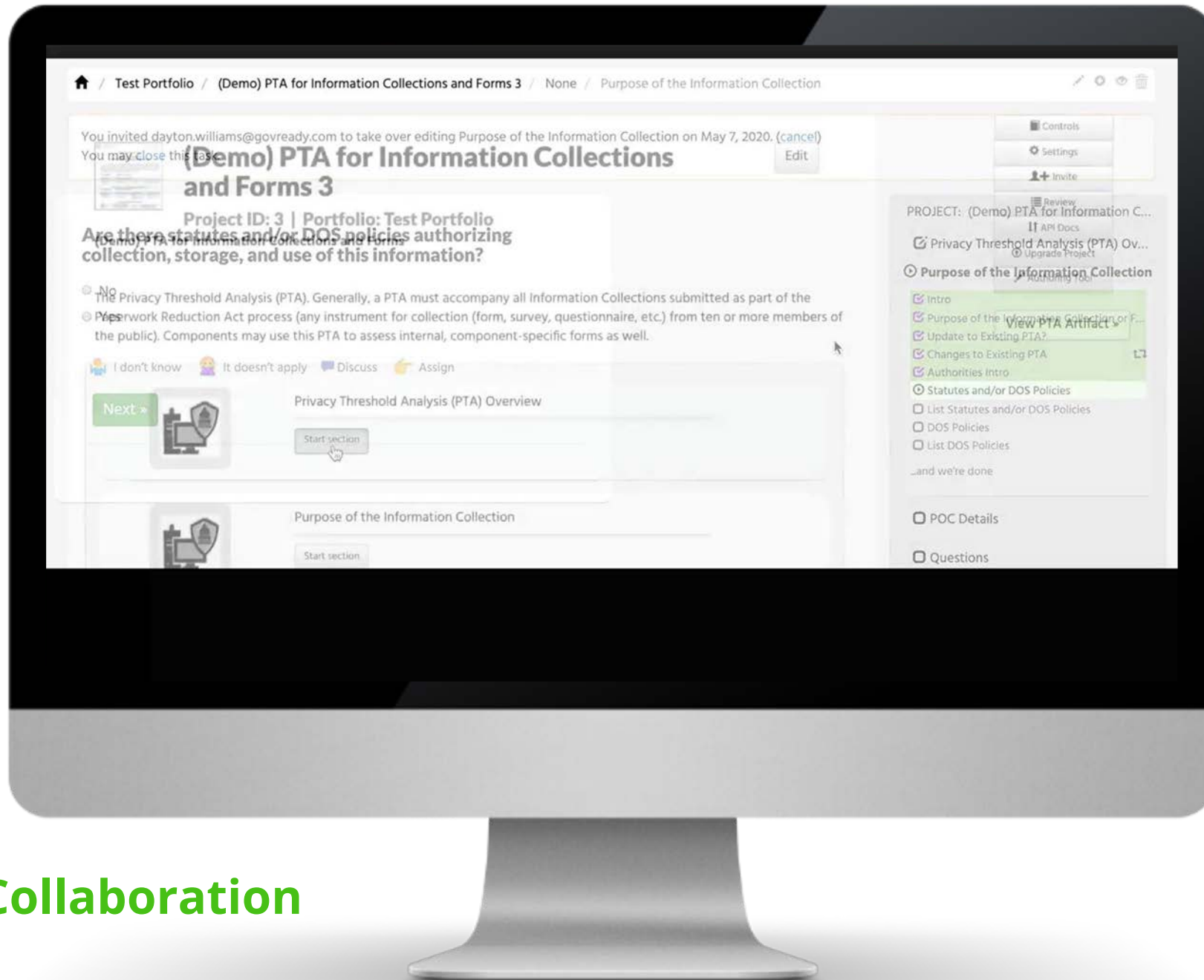
Security Control Status

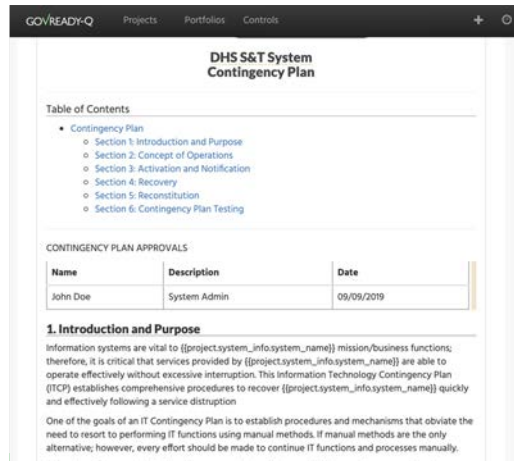
Control implementation now tracked directly in database instead of questionnaires enabling richer metadata management including control status.

03

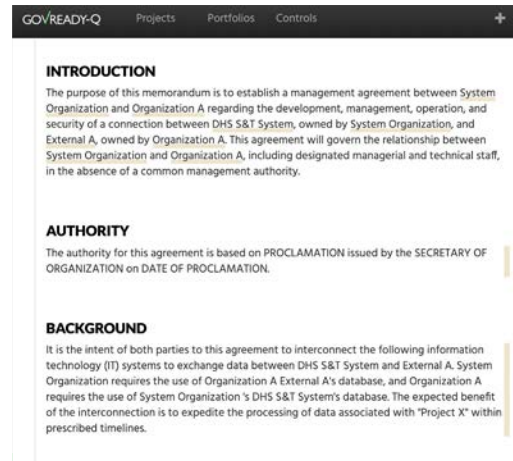
Next Tasks

Project display redesigned for better linear representation of modules and to dynamically show and hide modules to make next tasks clearer.

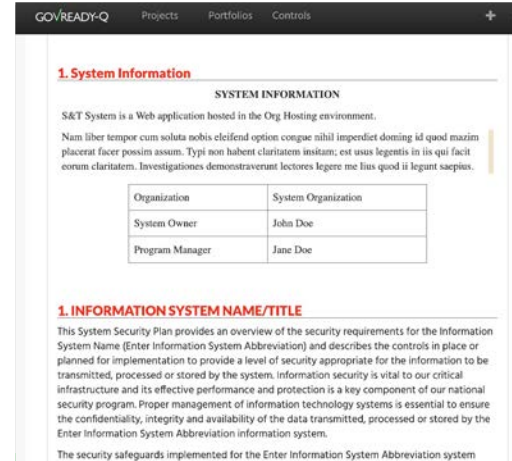




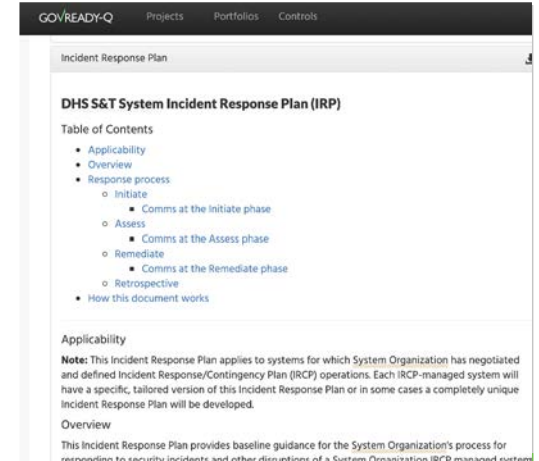
Contingency Plan (CP)



Memorandum of Understanding (MOU)



System Security Plan (SSP)



Incident Response Plan (IRP)

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.