

GovReady®

Making Compliance Easier
gregelin@govready.com

**What does a working
OSCAL Component Library
Really Look Like?**

NIST 2nd OSCAL Workshop, Feb 2021

GovReady Open Source GRC

Making Compliance Easier

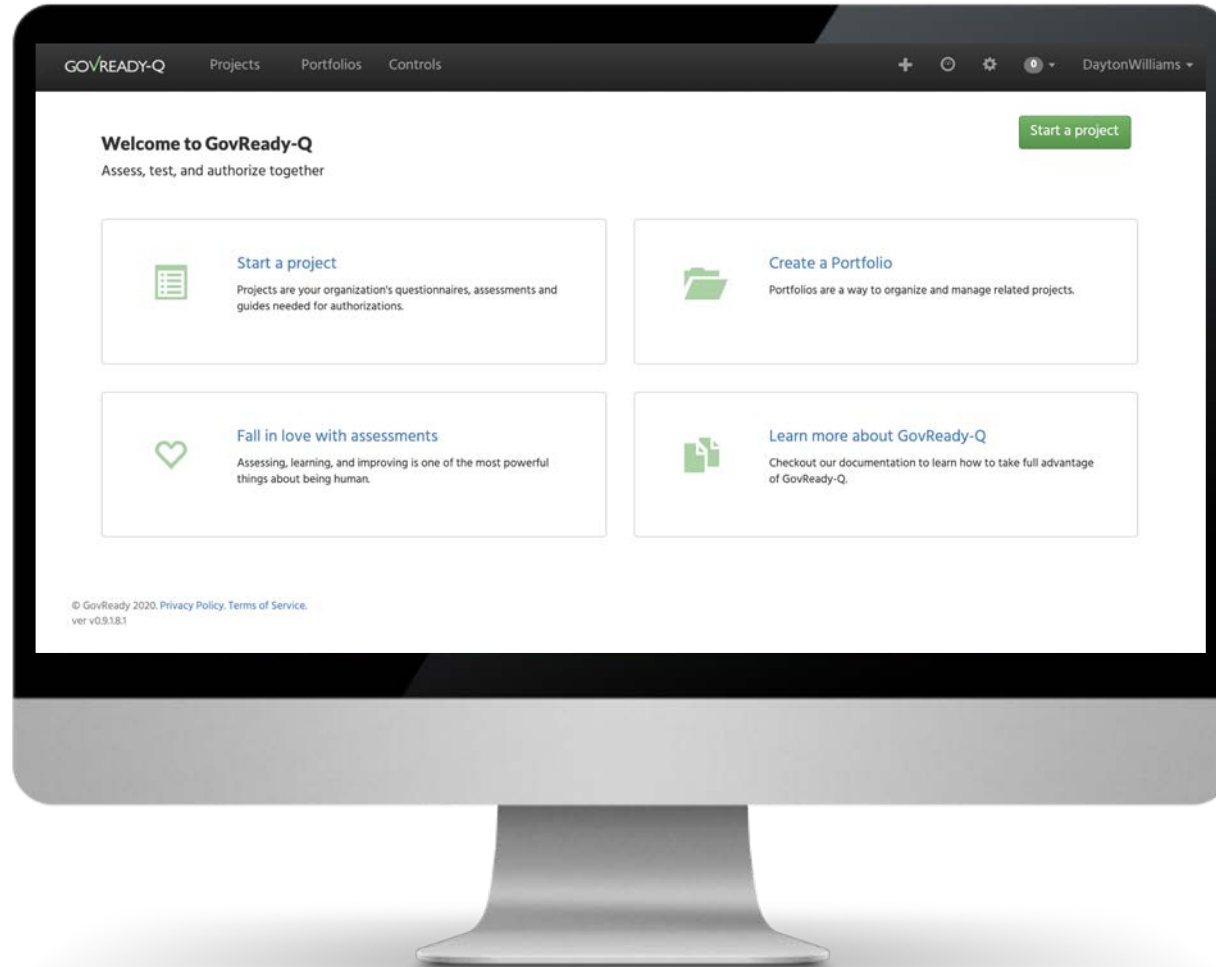
User Focus → User Friendly

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

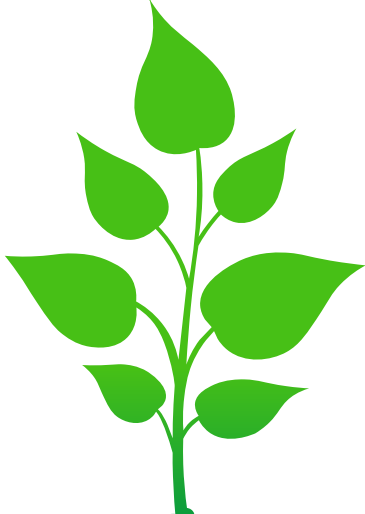
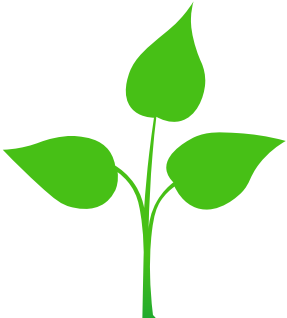
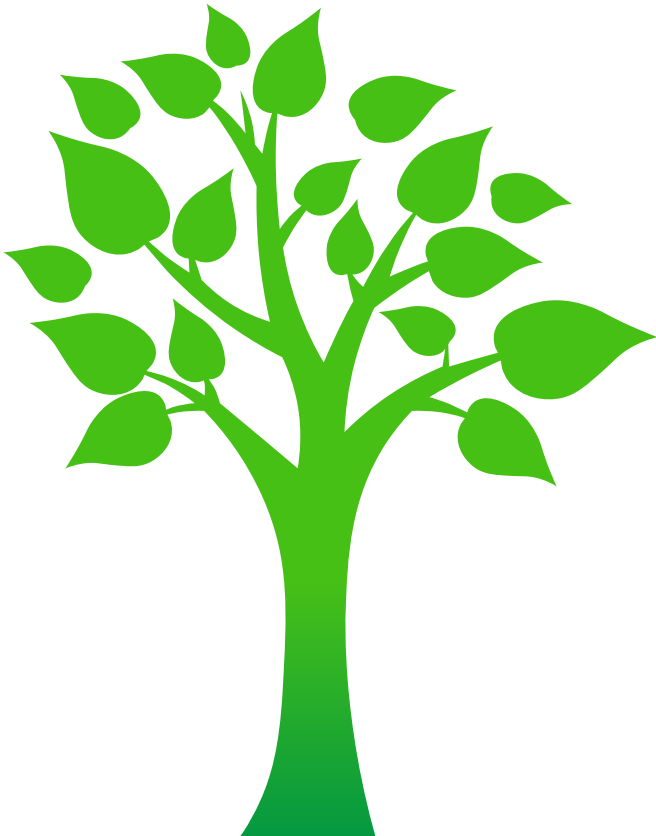
- Supports database encryption
- Supports FIPS 140-2 certified systems
- HTTPS TLS encrypted sessions
- Single Sign On (Proxy Authentication)
- Granular Access Control



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

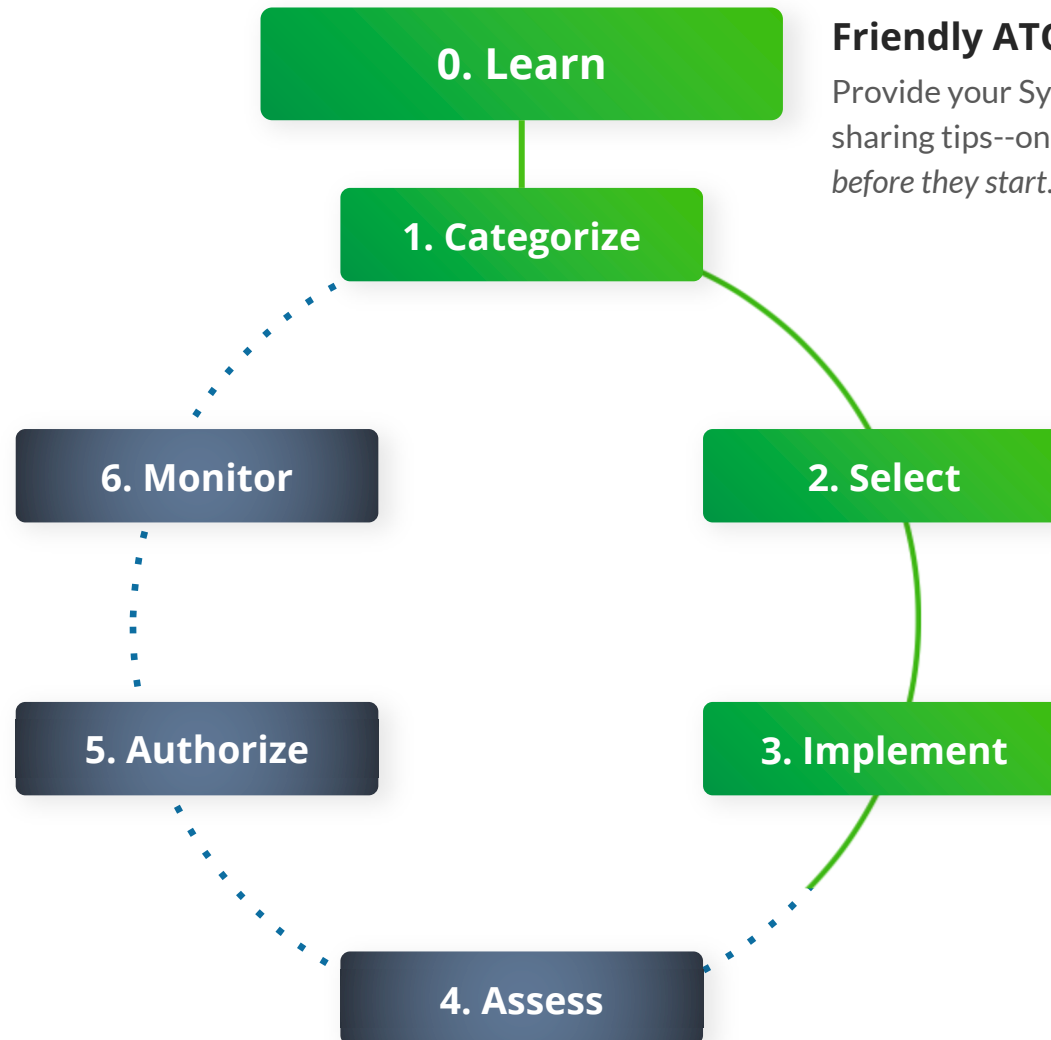
Early Adopters

- 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

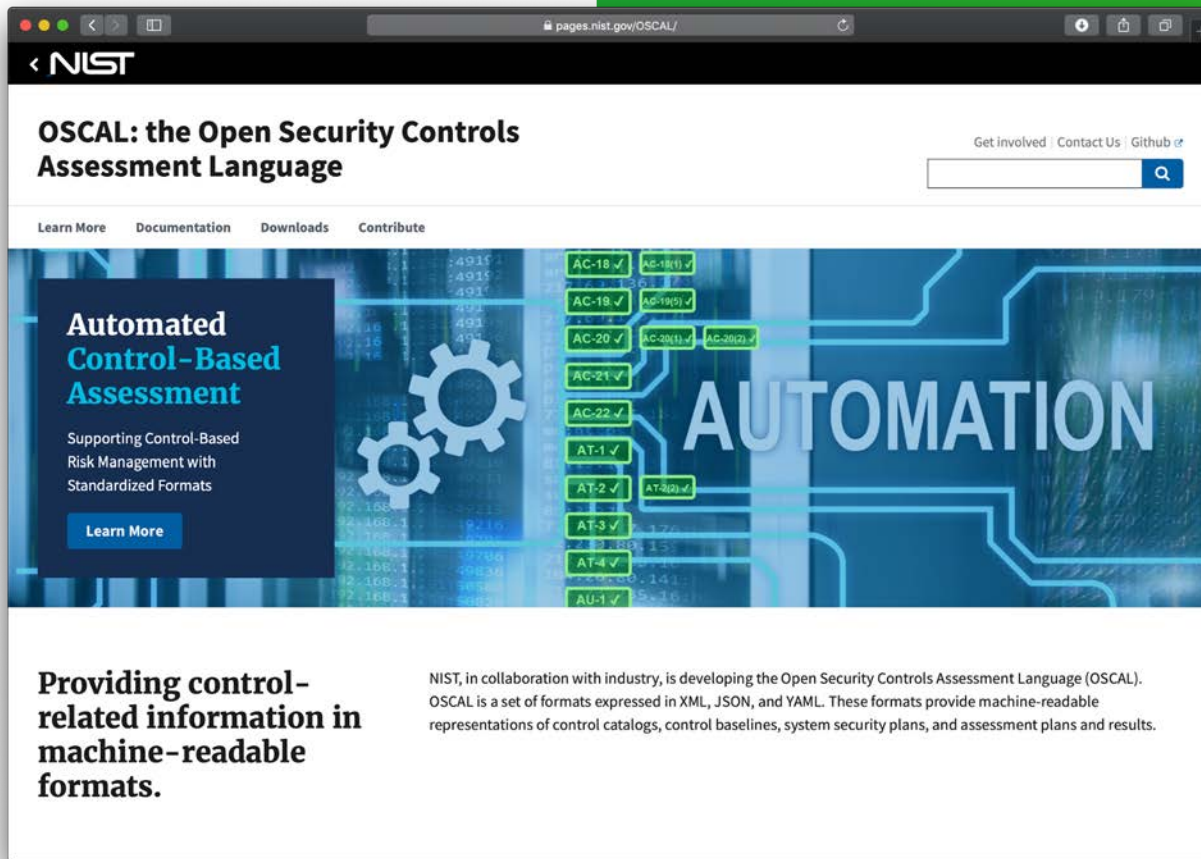
GovReady controls catalogs use NIST OSCAL format under the hood.

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 graphic with the word 'AUTOMATION' and a list of control IDs: AC-18, AC-19, AC-20, AC-21, AC-22, AT-1, AT-2, AT-3, AT-4, and AU-1. A sidebar on the left highlights 'Automated Control-Based Assessment' with a 'Learn More' button. Below the graphic, there is a section titled 'Providing control-related information in machine-readable formats.' followed by a paragraph explaining OSCAL.

OSCAL: the Open Security Controls Assessment Language

Get involved | Contact Us | Github

Learn More | Documentation | Downloads | Contribute

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.

Download SSP OSCAL JSON

The image shows a web application interface on the left and a code editor on the right. The web application is titled "GOVREADY-Q" and shows a breadcrumb path: "CustomerX / Test IT System / System Security Plan". Under the heading "...and we're done", there is a section for "Available documents" with a table of download options:

Document	Downloads
SSP v1	Word (docx) Open Office (odt) HTML Markdown Plain Text
SSP v1 (OSCAL/JSON)	OSCAL (json)
SSP v1 (OSCAL/XML)	OSCAL (xml)

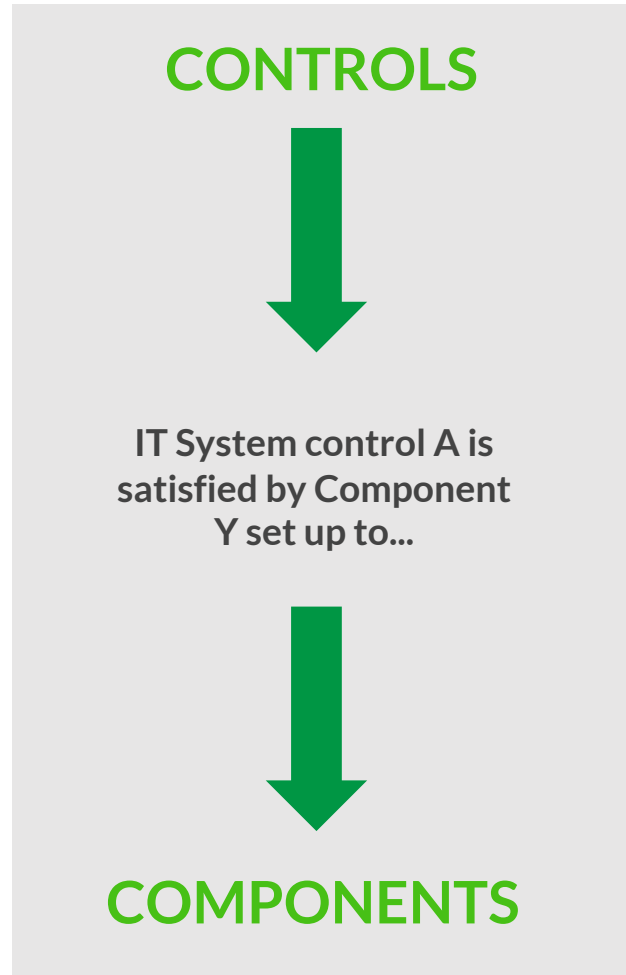
Below this is a "Your Answers" section with a "Question" and "Answer" header, and a message: "No questions needed to be answered in this section." At the bottom, there are three buttons: "Continue to ATO Letter »" (green), "Return to project", and "Review »".

The code editor on the right shows the content of the "ssp_v1_oscal_json.json" file. The JSON structure includes:

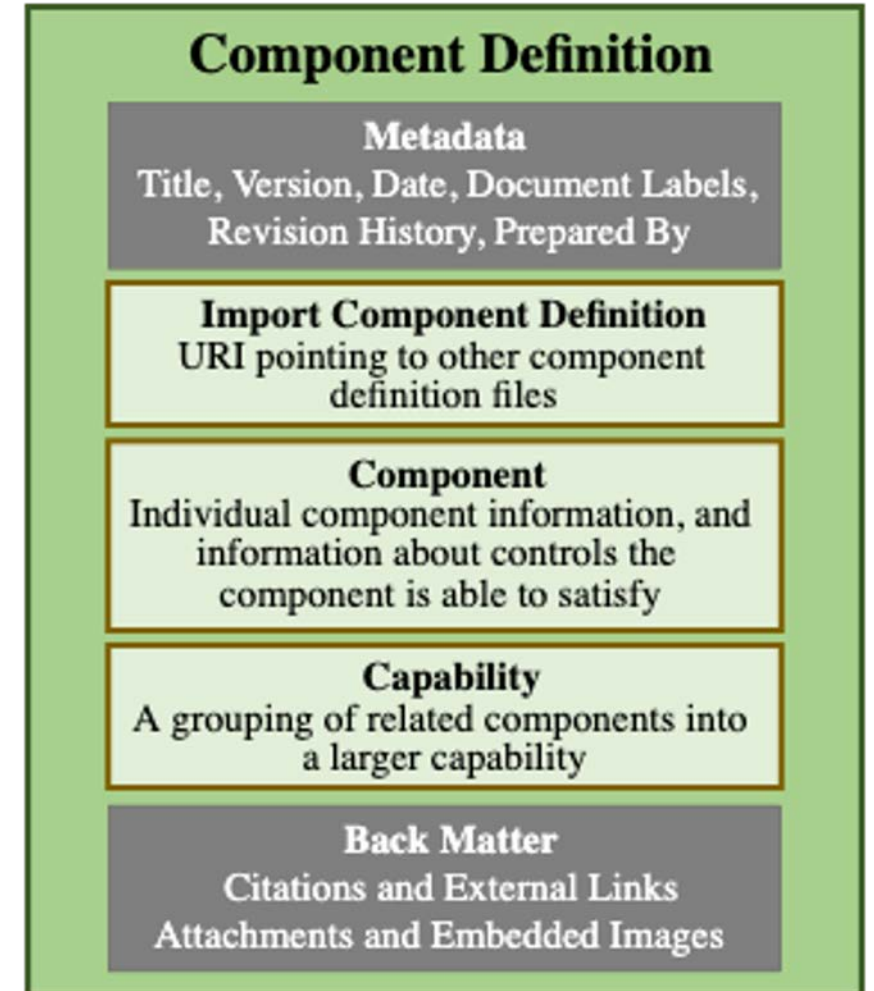
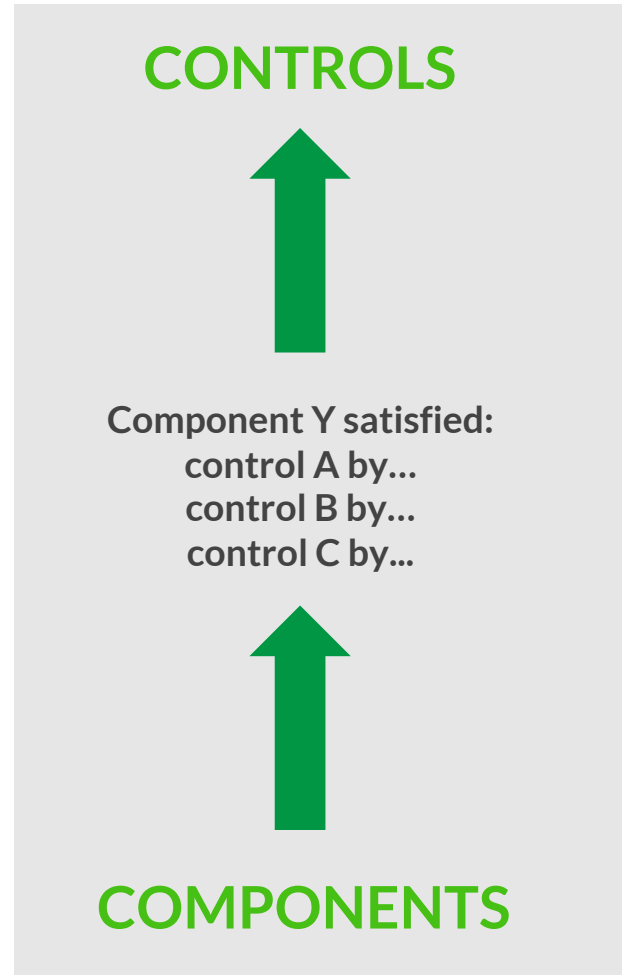
- `system-security-plan`: Metadata such as `uid`, `title`, `last-modified`, `version`, and `oscal-version`.
- `import-profile`: Reference to a profile path.
- `system-characteristics`: `system-ids` array containing `govready-75`.
- `system-name`: `CustomerX Website`, `system-name-short`: `CXW`.
- `description`: "This system supports CustomerX Website\."
- `security-sensitivity-level`: `<FISMA Level>`.
- `system-information`: Array of information types with `title`, `description`, and `confidentiality-impact`.
- `integrity-impact` and `availability-impact`: Information type impacts.
- `security-impact-level`: `security-objective-confidentiality`, `security-objective-integrity`, and `security-objective-availability` all set to `UNKNOWN`.
- `status`: `state` is `operational`.
- `authorization-boundary`: `description` is `System authorization boundary, TBD`.
- `system-implementation`: `users` and `components` arrays.

Impact of Component Library

Traditional Top Down
Hard to reuse



CAC Bottom Up
Easier to reuse



What Features Make a **Component Library**

Essential

Distinct Library
View Components
Read Component
Update Component
Select Components
Delete Component

Better

Compare (Diff) Components
Export Component
Import Component(s)
Manage “Certification”

Best

Manage Imports
Import in Projects

Component Library

The screenshot shows a web browser window with the URL `test.govready.com/controls/components`. The browser's address bar and tabs are visible at the top. The page header includes the "GOVREADY-Q" logo and navigation links for "Projects", "Portfolios", "Controls", "Component Library", and "App Library". On the right side of the header, there are icons for a plus sign, a refresh button, a settings gear, a notification bell with "6" items, and a user profile labeled "admin".

Below the header, there are three green buttons: "Manage Import Records", "Create a Component", and "Import OSCAL Component".

The main content area is titled "Component Library" and includes the text "You have access to 40 components." Below this is a table titled "Available Components" with three columns: Component Name, Description, and Number of Statements.

Available Components		
2 Twelve E3 Labs (System)	The entire 2 Twelve E3 Labs General Support Service	301 statements
2 Twelve E3Lab	<i>No description provided.</i>	4 statements
2 Twelve E3Lab	<i>No description provided.</i>	1 statement
2 Twelve Responsibility	<i>No description provided.</i>	1 statement
AWS Cloud Formation	<i>No description provided.</i>	2 statements
AWS IAM	<i>No description provided.</i>	1 statement
Acceptable Uses and Exports for Users of NGA Systems	A user account policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, typically within an organization. It is very important for large sites where users typically have accounts on ma	1 statement
Agency ICAM Single Sign On	<i>No description provided.</i>	1 statement
Agency Office of Information & Technology	<i>No description provided.</i>	1 statement
Ansible Tower	<i>No description provided.</i>	1 statement

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 'AC-3 Access Enforcement' is displayed, with 'NIST SP-800-53 rev4' as a sub-header. A navigation bar below the sub-header contains tabs for 'Control', 'Component Statements' (with a '2' indicator), 'Combined Statement', 'OSCAL', and 'OpenControl'. The 'Component Statements' tab is currently selected.

Under the 'Component Statements' tab, the heading 'Component Implementations Statements' is followed by two implementation cards:

- 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 of the page, there is a form for adding a component. It includes a green 'Add existing component' button, a text input field for 'Name of component', a dropdown menu with 'Test Cmp Name modified' selected, and a green 'Submit for related' button. Below this is another green button labeled 'Add component statement'.

A footer note at the bottom left reads: 'Open #component_controls on this page in a new tab'.

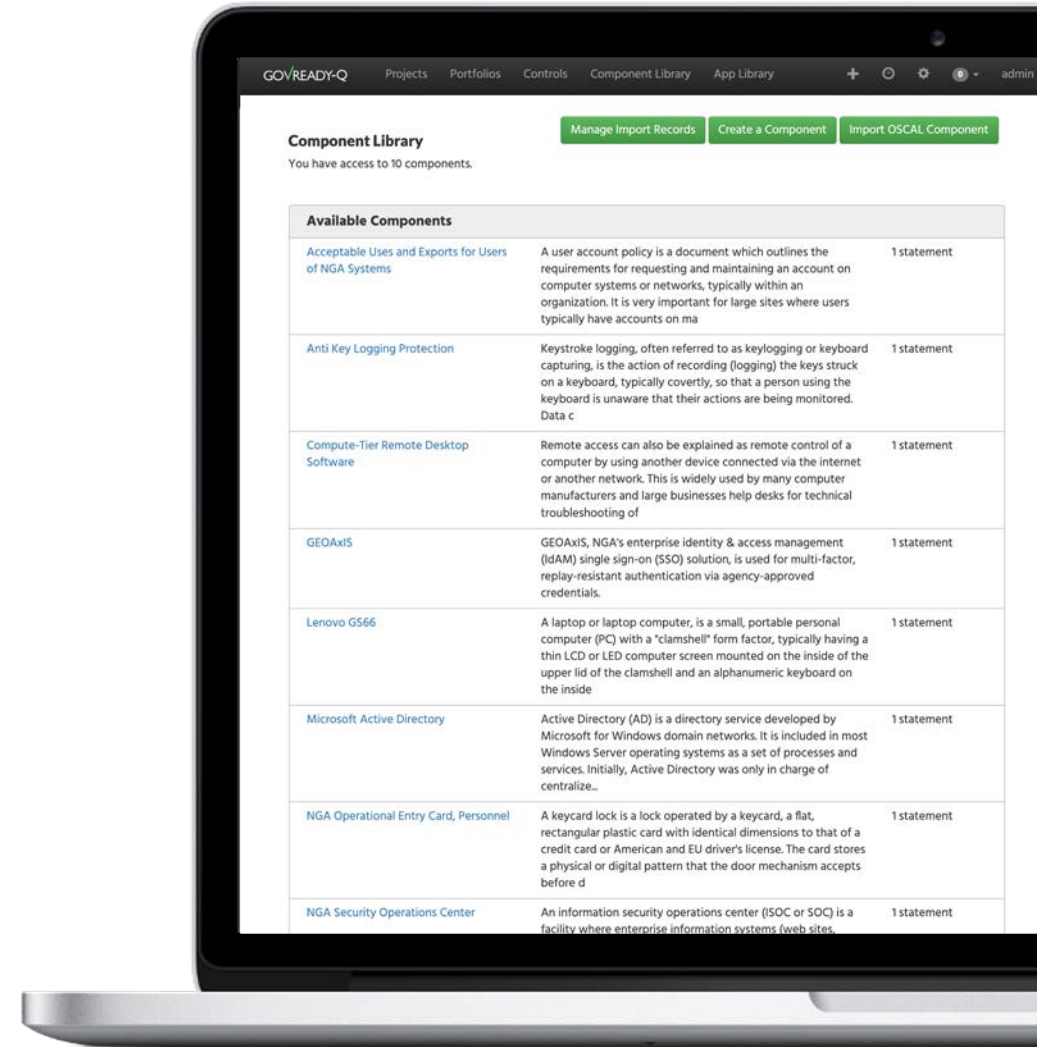
DEMO

Demo of Making an SSP



Links Open Source OSCAL Tools

- <https://govready.com>
Website
- <https://github.com/GovReady/govready-q>
GovReady GRC software
- <https://github.com/GovReady/CUB>
CAC Utility Belt scripts to generate OSCAL components from delimited files **NEW!**
- <https://github.com/GovReady/oscal-lifecycle-examples>
Community OSCAL examples **NEW!**



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

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

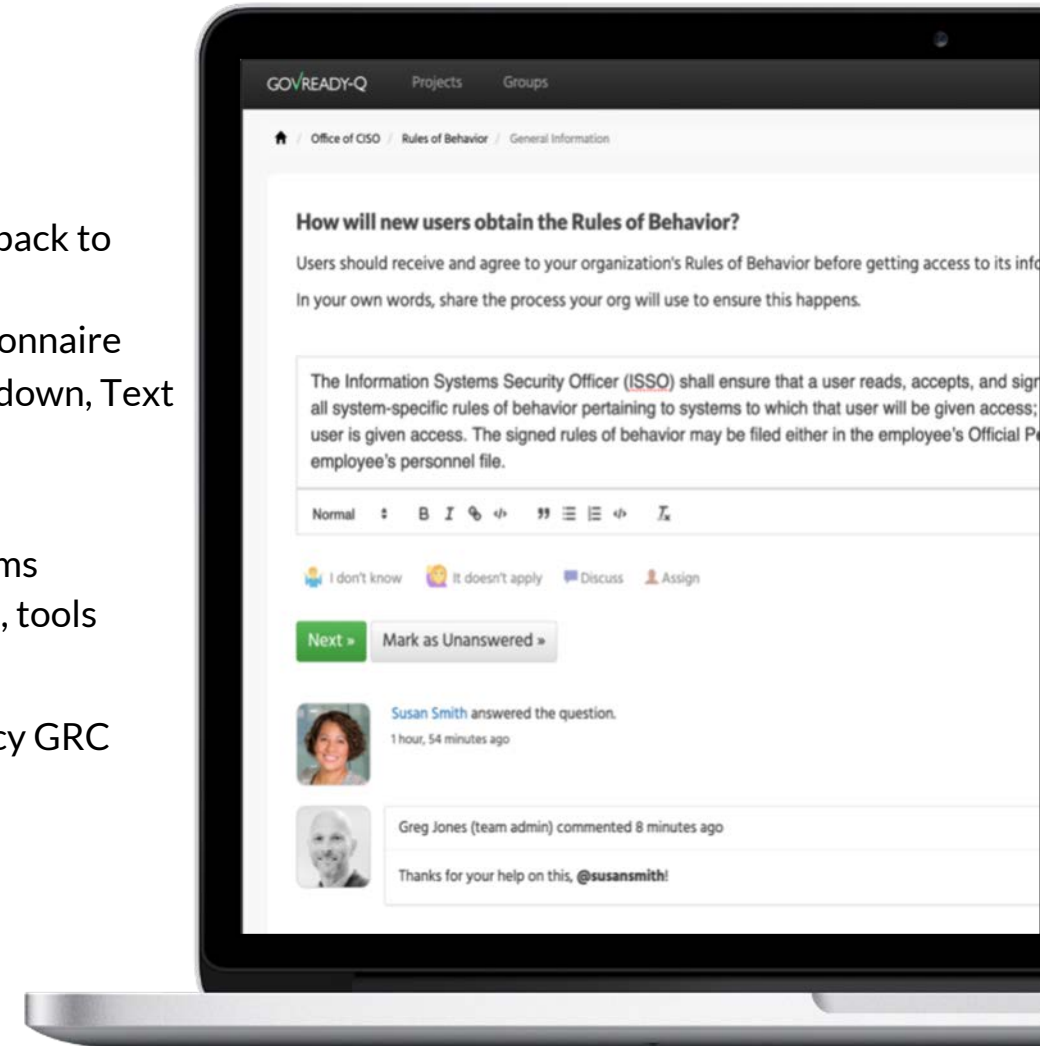
- Generate export data for legacy GRC

Enterprise-Ready

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

Customizable User Interface

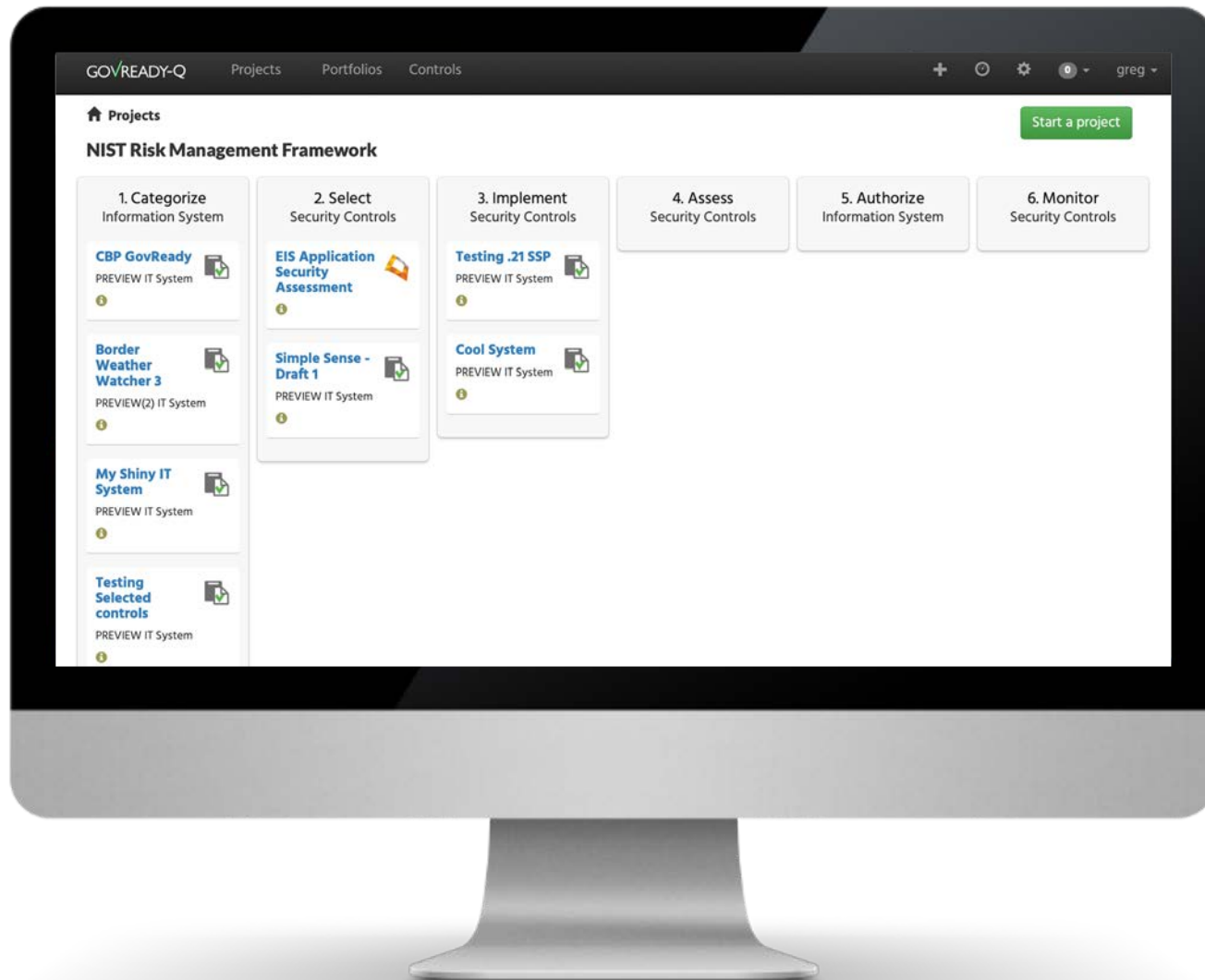
- Completely customizable UI to support organization look and feel
- Customize / Replace pages
- Aria-compatible components for 508 accessibility compliance



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

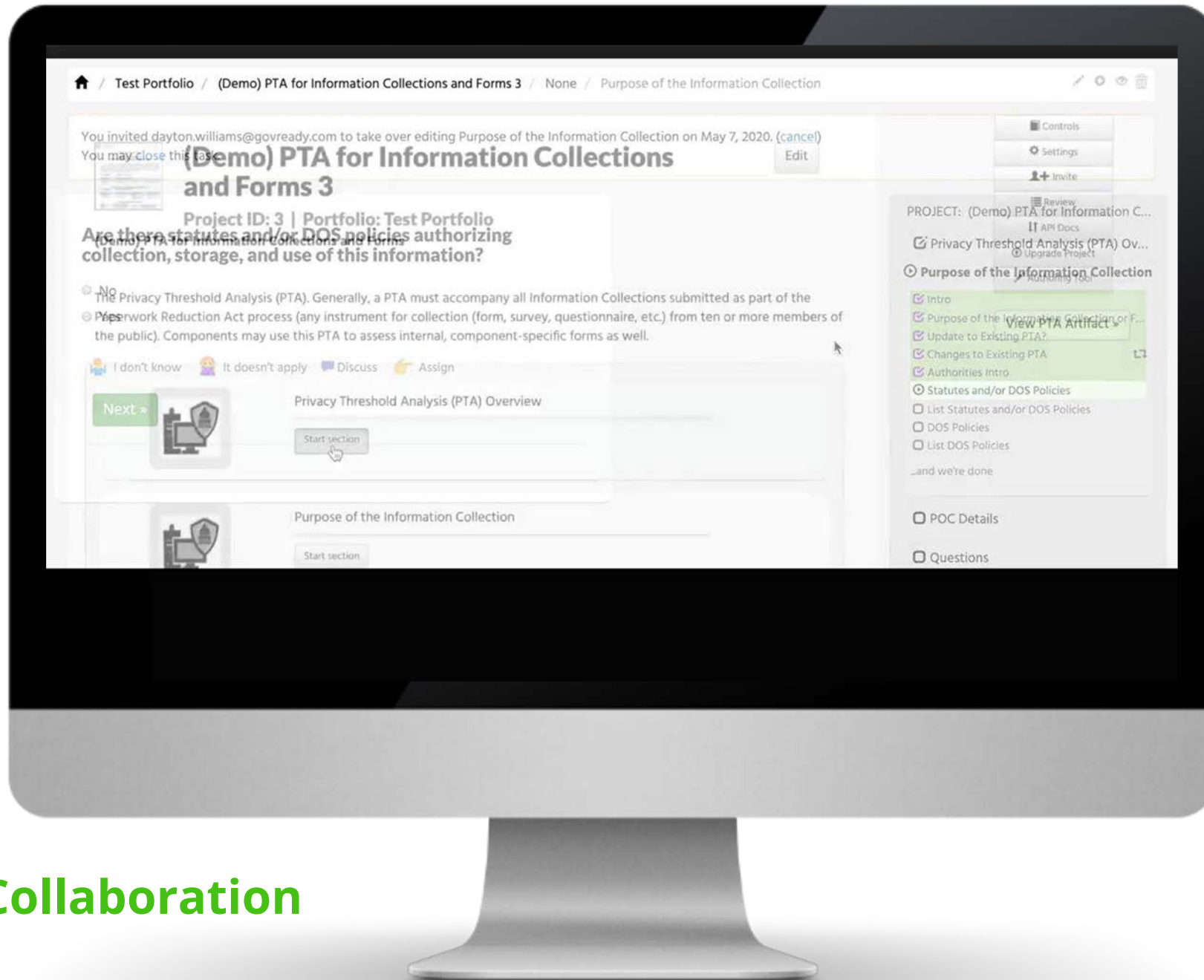
Security Control Status

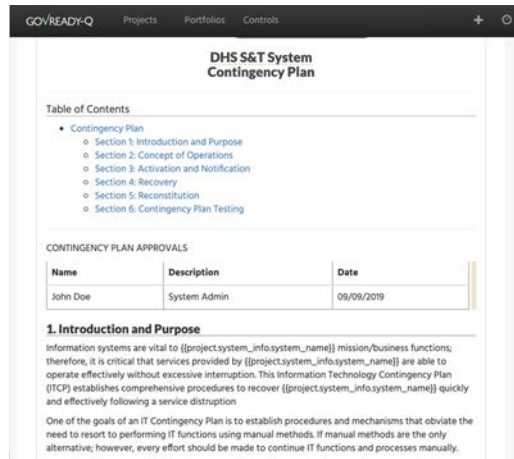
Control implementation now tracked directly in database instead of questionnaires enabling richer metadata management including control status.

03

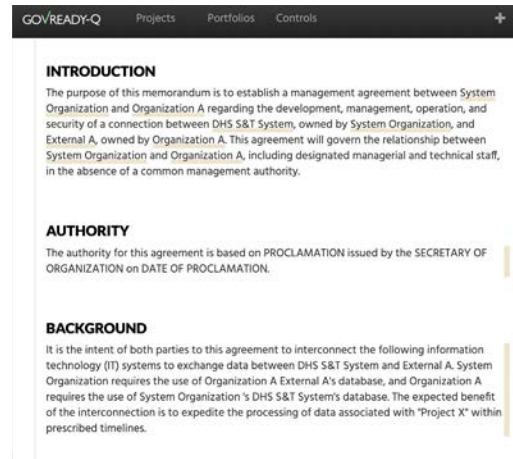
Next Tasks

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

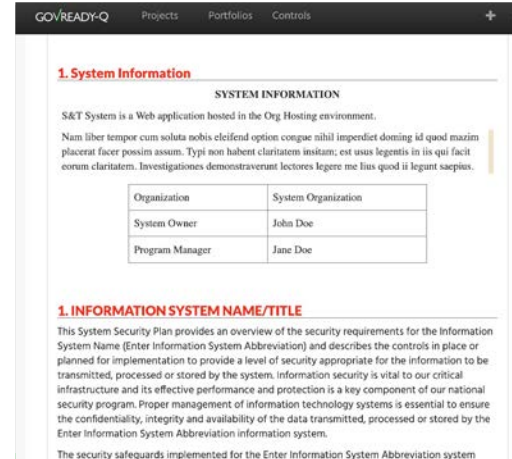




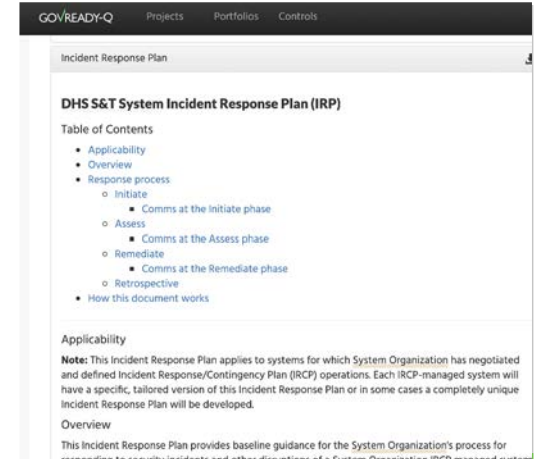
Contingency Plan (CP)



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.