The Joy of Open, Agile Government Security Compliance

Using F/LOSS, Agile and DevSecOps to help make compliance secure

Fen Labalme

CivicActions

TOC

- ➔ How did I get here
- ➔ What is CivicActions
- ➔ What is compliance
- ➔ Making compliance fun
- ➔ Culture of Security
- ➔ Next steps

How did I get here

Always had an interest in privacy and security

CivicActions

Fen's backstory

- ➔ 1977 Ron Rivest & Adi Shamir
- ➔ 1981 NewsPeek (social media)
- ➔ 1983 Broadcatch
- ➔ 1986 WELL Peace host, EFF
- ➔ 1992 Cypherpunks, General Magic
- ➔ 1994 P3P, XRI, IDCommons
- ➔ 2005 CivicActions...

Fen's backstory

- 1977 Ron Rivest & Adi Shamir
- **1981 NewsPeek (social media)**
- 1983 Broadcatch
- 1986 WELL Peace host, EFF
- 1992 Cypherpunks, General Magic
- 1994 P3P, XRI, IDCommons
- 2005 CivicActions...

Fen's backstory

- 1977 Ron Rivest & Adi Shamir
- 1981 NewsPeek (social media)
- **1983 Broadcatch**
- 1986 WELL Peace host, EFF
- 1992 Cypherpunks, General Magic
- 1994 P3P, XRI, IDCommons
- 2005 CivicActions...

Fen's backstory

- 1977 Ron Rivest & Adi Shamir
- 1981 NewsPeek (social media)
- 1983 Broadcatch
- **1986 WELL Peace host, EFF**
- 1992 Cypherpunks, General Magic
- 1994 P3P, XRI, IDCommons
- 2005 CivicActions...

Fen's backstory

- 1977 Ron Rivest & Adi Shamir
- 1981 NewsPeek (social media)
- 1983 Broadcatch
- 1986 WELL Peace host, EFF
- **1992 Cypherpunks, General Magic**
- 1994 P3P, XRI, IDCommons
- 2005 CivicActions...

Fen's backstory

- 1977 Ron Rivest & Adi Shamir
- 1981 NewsPeek (social media)
- 1983 Broadcatch
- 1986 WELL Peace host, EFF
- 1992 Cypherpunks, General Magic
- **1994 P3P, XRI, IDCommons**
- 2005 CivicActions...

Fen's backstory

- 1977 Ron Rivest & Adi Shamir
- 1981 NewsPeek (social media)
- 1983 Broadcatch
- 1986 WELL Peace host, EFF
- 1992 Cypherpunks, General Magic
- 1994 P3P, XRI, IDCommons
- **2005 CivicActions...**

What is CivicActions?

Holistic digital government services using human-centered design, Drupal, open data and agile/DevSecOps practices

CivicActions

- 2004 CivicActions founded
  - Berkeley founders, 100% remote work
- 10 years: Empowering at the Edges
  - Amnesty International, Greenpeace, ...
- 2014 Transforming Government
  - DSCA (DoD) was our first federal client

CivicActions

- ➔ 2004 CivicActions founded
  - ◆ Berkeley founders, 100% remote work
- ➔ **10 years: Empowering at the Edges**
  - ◆ **Amnesty International, Greenpeace, ...**
- ➔ 2014 Transforming Government
  - ◆ DSCA (DoD) was our first federal client

CivicActions

- ➔ 2004 CivicActions founded
  - ◆ Berkeley founders, 100% remote work
- ➔ 10 years: Empowering at the Edges
  - ◆ Amnesty International, Greenpeace, ...
- ➔ **2014 Transforming Government**
  - ◆ **DSCA (DoD) was our first federal client**

CivicActions

Agencies served include:

- ➔ Defense Security Cooperation Agency (DSCA)
- ➔ U.S. Department of Education (DoED)
- ➔ U.S. Department of Health and Human Services (HHS)
- ➔ National Science Foundation (NSF)
- ➔ Federal Communications Commission (FCC)
- ➔ U.S. Department of Veteran Affairs (VA)
- ➔ San Francisco Department of the Environment (SFE)
- ➔ U.S. General Services Administration (GSA)
- ➔ Smithsonian Museum of Natural History

What is this “Compliance”?

A condensed history of how federal compliance got here

CivicActions

Federal Compliance

Origins

- 1995 British Standard BS 7799
  - *Code of practice for information security management*
- 1996 HIPAA
- 2002 SOX (Sarbanes-Oxley)
- 2004 PCI DSS v1
- 2005 BS 7799 adopted as ISO 27000 (latest revision in 2013)

Federal Compliance Origins

- 1995 British Standard BS 7799
  - *Code of practice for information security management*
- **1996 HIPAA**
- 2002 SOX (Sarbanes-Oxley)
- 2004 PCI DSS v1
- 2005 BS 7799 adopted as ISO 27000 (latest revision in 2013)

Federal Compliance Origins

- 1995 British Standard BS 7799
  - *Code of practice for information security management*
- 1996 HIPAA
- 2002 SOX (Sarbanes-Oxley)
- 2004 PCI DSS v1
- 2005 BS 7799 adopted as ISO 27000 (latest revision in 2013)

Federal Compliance Origins

- 1995 British Standard BS 7799
  - *Code of practice for information security management*
- 1996 HIPAA
- 2002 SOX (Sarbanes-Oxley)
- **2004 PCI DSS v1**
- 2005 BS 7799 adopted as ISO 27000 (latest revision in 2013)

Federal Compliance Origins

- 1995 British Standard BS 7799
  - *Code of practice for information security management*
- 1996 HIPAA
- 2002 SOX (Sarbanes-Oxley)
- 2004 PCI DSS v1
- **2005 BS 7799 adopted as ISO 27000 (latest revision in 2013)**

Federal Compliance Origins

2002 - FISMA became law

Federal Information Security Management Act

- ➔ The process takes 9-18 months, $600K-$1.5m
- ➔ Grants a 3-year “Authority to Operate” (ATO)

Federal Compliance

Origins

- ➔ 2013 - CDM : *Continuous Diagnostics and Mitigation* (“Continuous Monitoring”)
- ➔ 2014 - FISMA (modernization)
- ➔ 2015 - NIST 800-53r4 : *Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems: a Security Life Cycle Approach*

Federal Compliance Origi

Federal Compliance Origins

CDM monitoring agents are generally designed for Windows & proprietary software (Microsoft or McAfee)

OK, maybe
I'm a little biased

Federal Compliance Origins

- 2013 - CDM : *Continuous Diagnostics and Mitigation* (“Continuous Monitoring”)
- 2014 - FISMA (modernization)
- 2015 - NIST 800-53r4 : *Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems: a Security Life Cycle Approach*

Federal Compliance Origins

- 2013 - CDM : *Continuous Diagnostics and Mitigation* (“Continuous Monitoring”)
- 2014 - FISMA (modernization)
- **2015 - NIST 800-53r4 : *Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems: a Security Life Cycle Approach***

Federal Compliance Origins

18 Risk Management Framework (RMF) control families

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

What am I doing here?

Worlds collide: Fen becomes a CISO

CivicActions

Worlds collide

- ➔ 2015 CivicActions needed a CISO
- ➔ 2016 I wrote my first SSP for a DoD ATO using FISMA/RMF methods
  - ◆ 400 page word doc with screenshots for evidence
  - ◆ Vowed to never do that again

Worlds collide

- 2015 CivicActions needed a CISO
- **2016 I wrote my first SSP for a DoD ATO using FISMA/RMF methods**
  - 400 page word doc with screenshots for evidence
  - Vowed to never do that again

Worlds collide

- ➔ 2015 CivicActions needed a CISO
- ➔ 2016 I wrote my first SSP for a DoD ATO using FISMA/RMF methods
  - ◆ **400 page word doc with screenshots for evidence**
  - ◆ Vowed to never do that again

CivicActions

Worlds collide

- 2015 CivicActions needed a CISO
- 2016 I wrote my first SSP for a DoD ATO using FISMA/RMF methods
  - 400 page word doc with screenshots for evidence
  - **Vowed to never do that again**

CivicActions

Updating Risk Management

Is the government actually doing the right thing?

CivicActions

Updating Risk Management

2016 - OMB Circular No. A-130

Managing Information as a Strategic Resource

- ➔ Defines "**ongoing authorization**" as "the means for determining risk and risk acceptance decisions"
- ➔ "Employ vulnerability scanning tools and techniques and promote **interoperability**…"

Updating Risk Management

2017 NIST Cybersecurity Framework (CSF)

- ➔ **Voluntary guidance**
- ➔ **Clear language** (readable by CEOs)
- ➔ Implemented **without government assistance**

Updating Risk Management

2018 - NIST 800-137v2 (RMFv2) changes

- ➔ "**Prepare**" step added to enable more effective and efficient risk management processes
- ➔ "**Privacy**" added to emphasize its critical role
- ➔ "**The Information Life Cycle"** describes the stages through which information passes
- ➔ **"Continuous monitoring"** well defined

Updating Risk Management

RMF v2 “privacy overlay”

- ➔ AP - Authority and Purpose
- ➔ AR - Accountability, Audit and Risk Management
- ➔ DI - Data Quality and Integrity
- ➔ DM - Data Minimization and Retention
- ➔ IP - Individual Participation and Redress
- ➔ SE - Security
- ➔ TR - Transparency
- ➔ UL - Use Limitation

Updating Risk Management

Cybersecurity scope is rapidly expanding

- ➔ Systems are virtualizing and moving to the cloud
- ➔ GDPR (General Data Protection Regulation) adopted April 2016
- ➔ CCPA (California Consumer Privacy Act of 2018) takes effect January 2020

Endpoint security improving

System Security Plans and ATOs are still too static

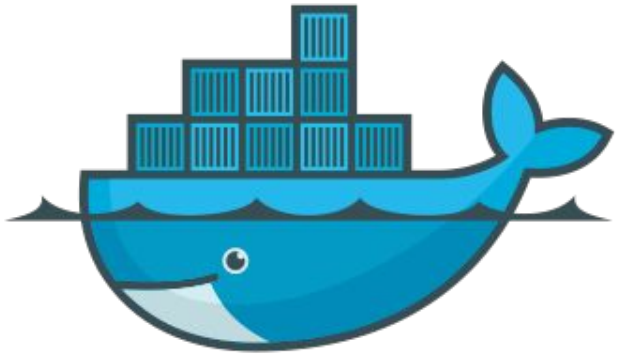
CivicActions

CivicActions

Making compliance fun

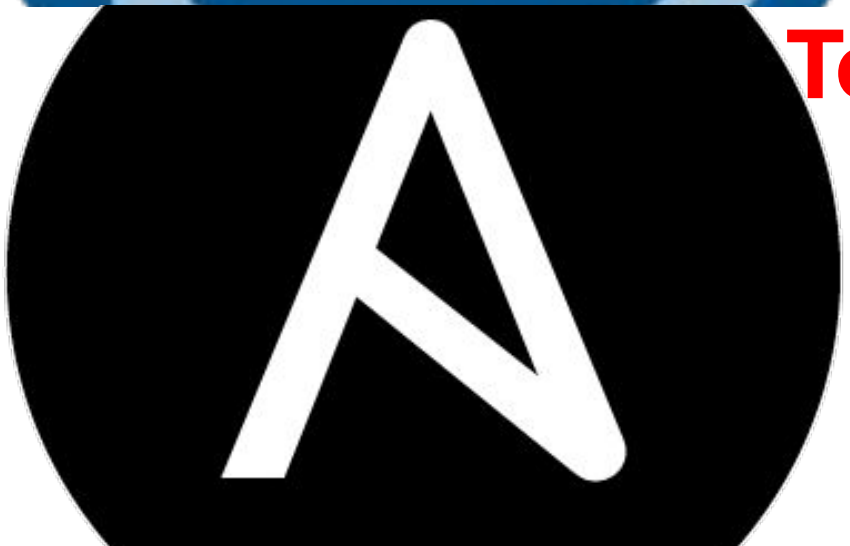
Path towards joy:
Automate the creation of the System Security Plan (SSP)

CivicActions



docker

Open Source Tools



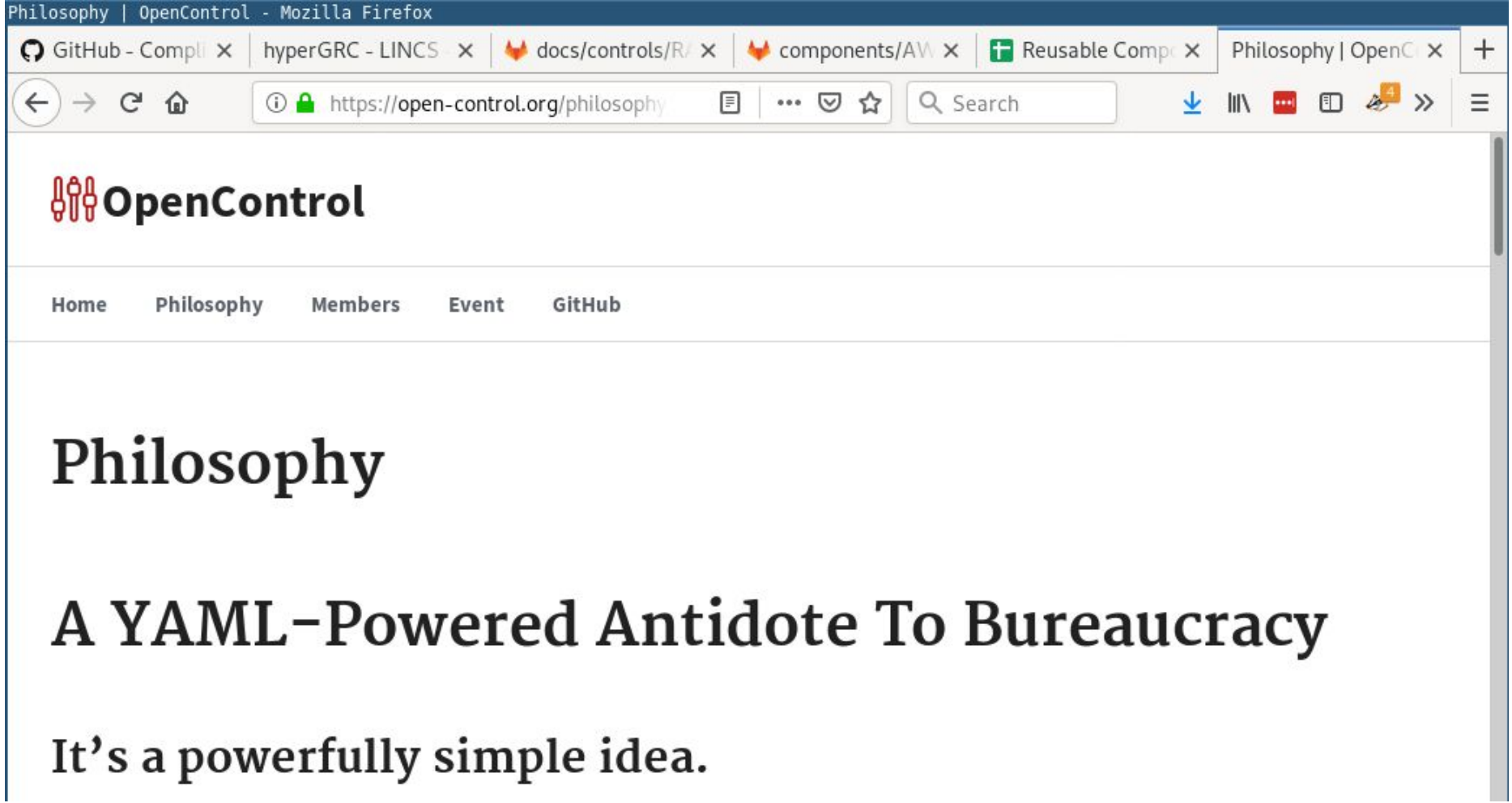
Key to LISaaS Baseline

There are six (6) categories of FedRAMP Tailored Low Impact-Software as a Service (LI-SaaS) Baseline controls, based on the FedRAMP Low Impact Baseline, that are required to be addressed by the Cloud Service Provider (CSP). The following table provides a list of the tailoring symbols with a short description of the tailoring criteria.

Tailoring Symbol	Tailoring Criteria
FED	Controls that are uniquely Federal, which are primarily the responsibility of the Federal Government
NSO	Controls FedRAMP determined. Does not impact the security of the Cloud SaaS
Required	Controls FedRAMP determined. Not required for Low Impact Cloud SaaS, and are independently assessed
Conditional	Controls FedRAMP determined to be conditionally required for Low Impact Cloud SaaS
Inherited	Controls FedRAMP determined to be inherited from the underlying infrastructure provider (i.e., FedRAMP authorized IaaS/PaaS) for Low Impact Cloud SaaS
Attestation	Controls for which FedRAMP determined that the CSP is required to attest to being in place for Low Impact Cloud SaaS

Automate the System Security Plan (SSP) creation

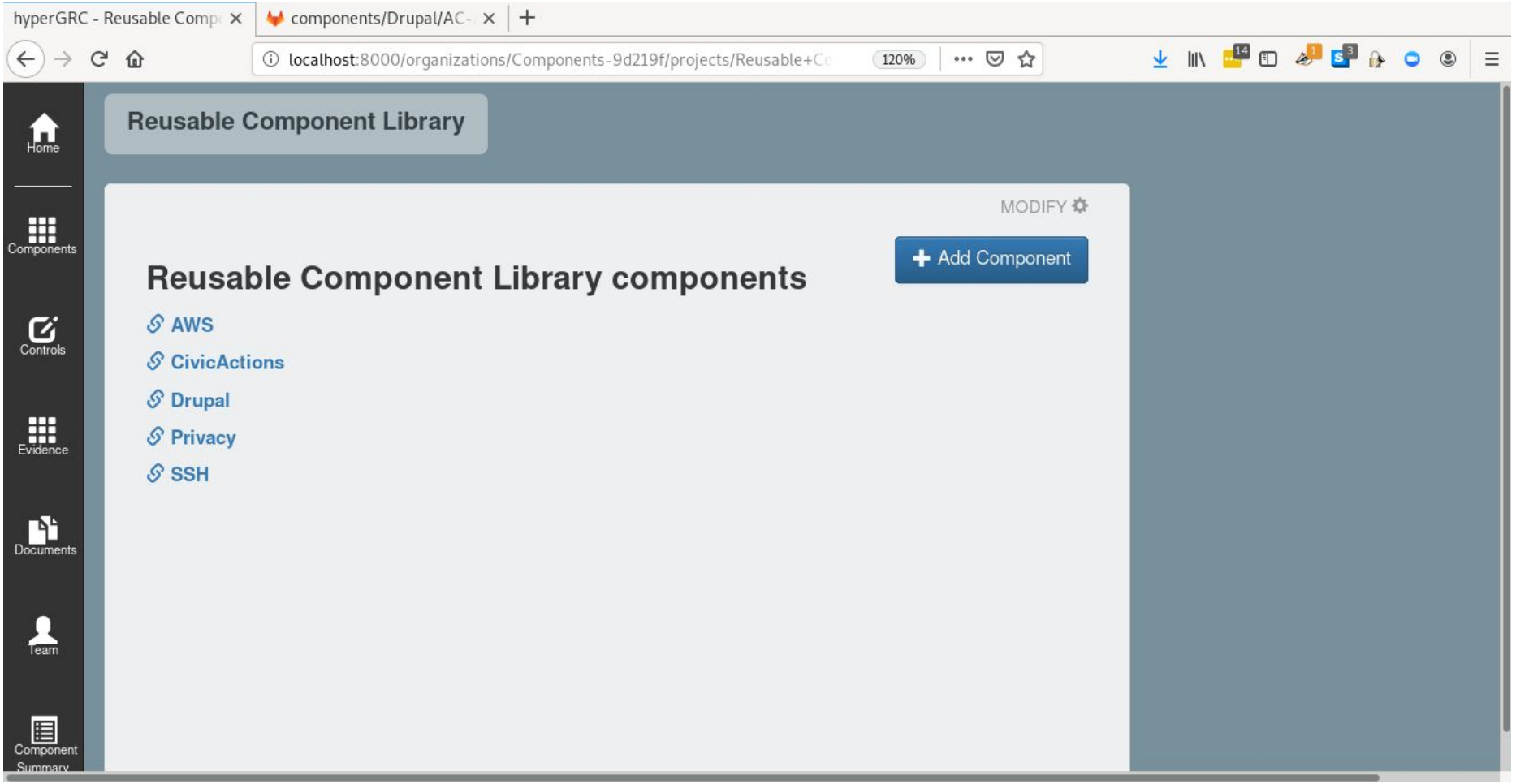
1. Sharing of control information
2. Reusable components
3. Machine readable OpenControl YAML files in git
4. Automated document creation
5. Automated evidence collection and control verification


Philosophy | OpenControl - Mozilla Firefox
GitHub - Compli
hyperGRC - LINCS
docs/controls/R
components/AW
Reusable Compo
Philosophy | OpenC
https://open-control.org/philosophy
Search
OpenControl
Home
Philosophy
Members
Event
GitHub
Philosophy
A YAML-Powered Antidote To Bureaucracy
It's a powerfully simple idea.

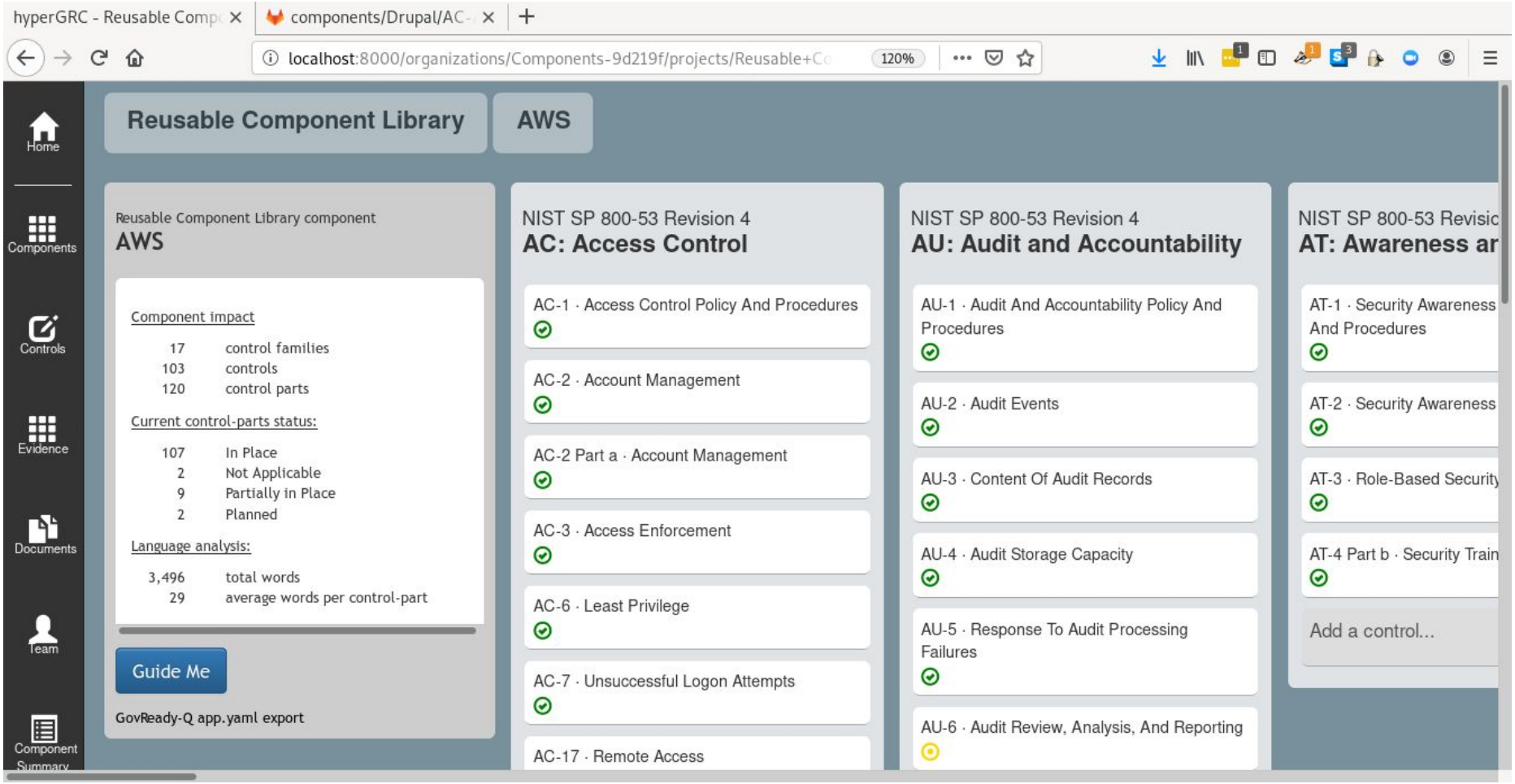

OSCAL Home | OSCAL - Mozilla Firefox
GitHub - Compli
hyperGRC - LINCS
docs/controls/R
components/AW
Reusable Compo
OSCAL Home |
https://pages.nist.gov/OSCAL/
Search
OSCAL: the Open Security Controls Assessment Language
Contact Us
Home
Learn More
Architecture
Downloads
Resources
Schema Reference
Community
F.A.S.T.
Assessment
Learn more about OSCAL
Fast, Accurate, Scalable,
Traceable: Documentary
Foundations for Systems Security
Get Involved
AC-17
AC-17(1)
AC-17(2)
AC-17(3)
AC-17(4)
AC-18
AC-18(1)
AC-19
AC-19(5)
AC-20
AC-20(1)
AC-20(2)
AC-21
AC-22
AT-1
AT-2
AT-2(2)
AT-3
AT-4
AUTOMATION

Automate the System Security Plan (SSP) creation

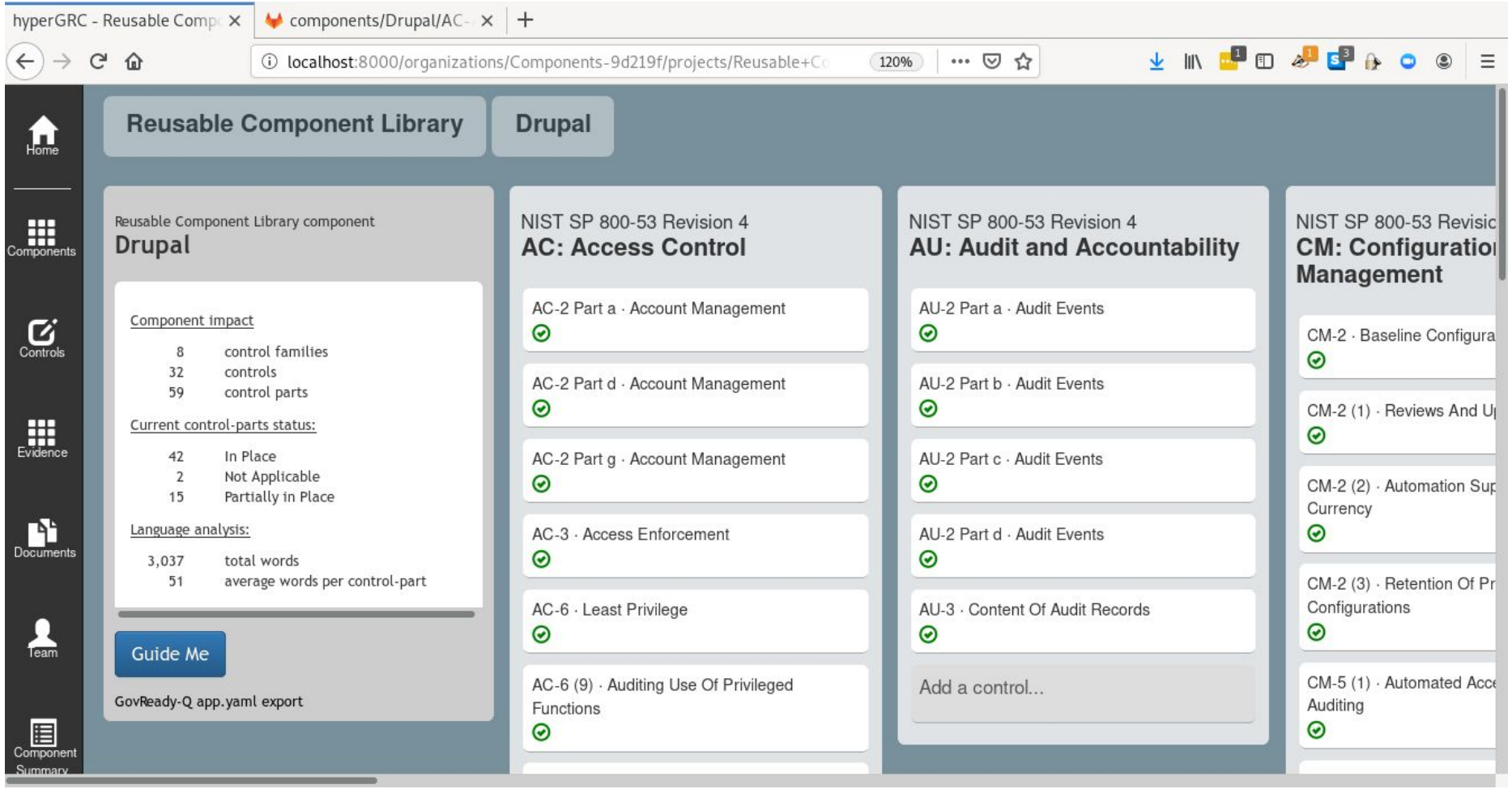
1. Sharing of control information
2. Reusable components
3. Machine readable OpenControl YAML files in git
4. Automated document creation
5. Automated evidence collection and control verification



CivicActions



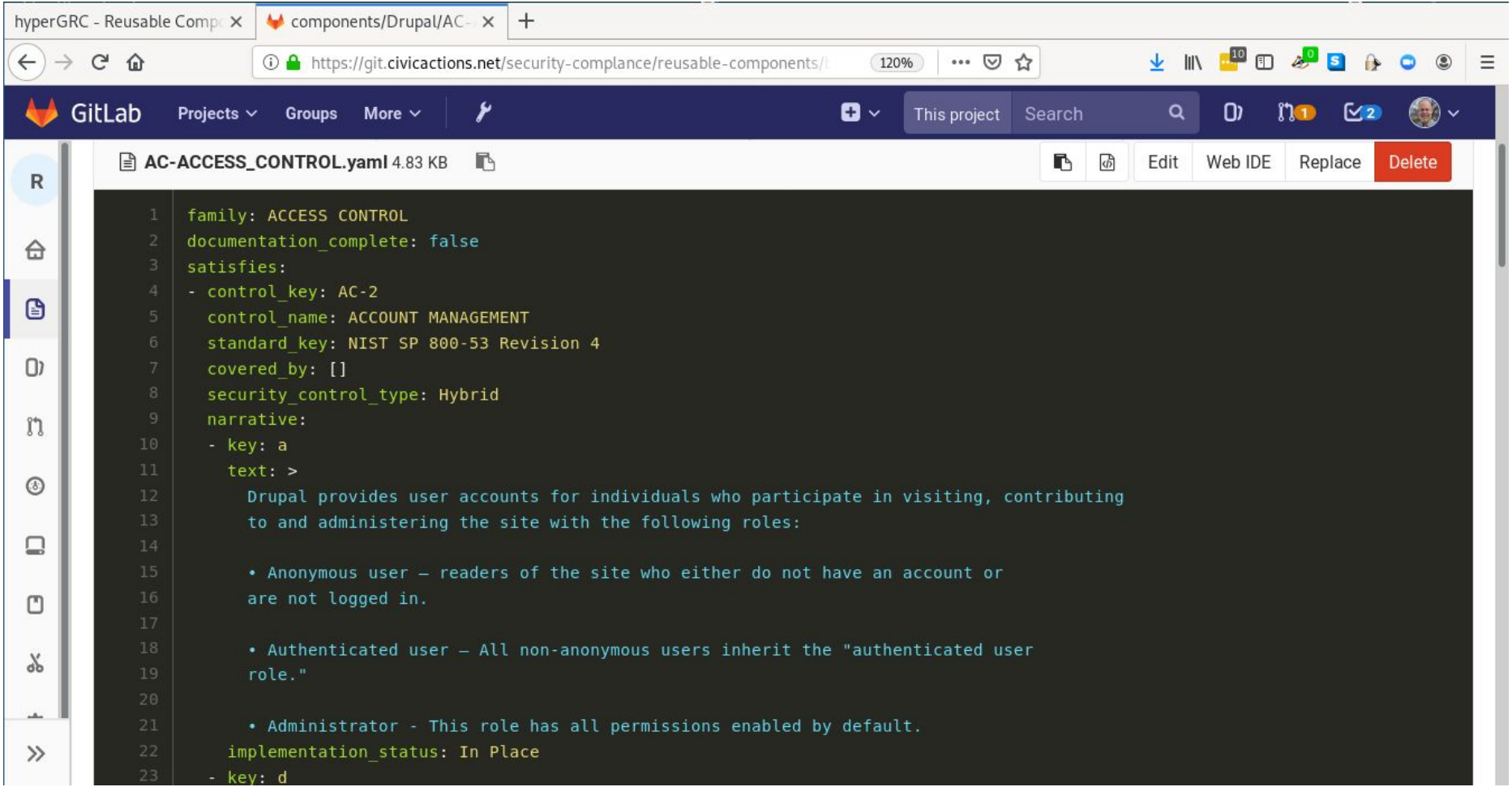
CivicActions

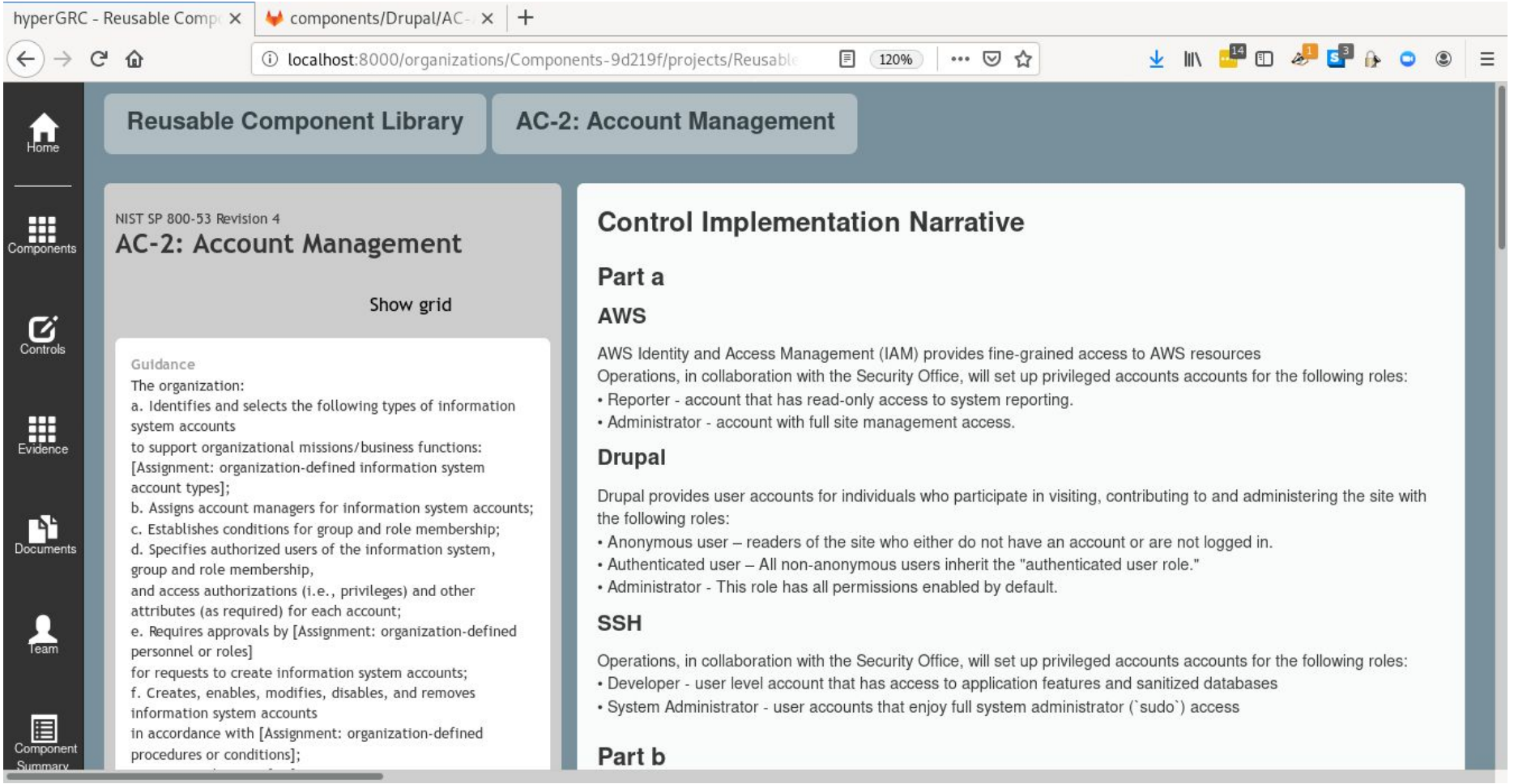


CivicActions

Automate the System Security Plan (SSP) creation

1. Sharing of control information
2. Reusable components
3. Machine readable OpenControl YAML files in git
4. Automated document creation
5. Automated evidence collection and control verification


hyperGRC - Reusable Comp
components/Drupal/AC-
https://git.civicactions.net/security-complance/reusable-components/
120%
GitLab
Projects
Groups
More
This project
Search
AC-ACCESS_CONTROL.yaml 4.83 KB
Edit
Web IDE
Replace
Delete
family: ACCESS CONTROL
documentation_complete: false
satisfies:
- control_key: AC-2
control_name: ACCOUNT MANAGEMENT
standard_key: NIST SP 800-53 Revision 4
covered_by: []
security_control_type: Hybrid
narrative:
- key: a
text: >
Drupal provides user accounts for individuals who participate in visiting, contributing
to and administering the site with the following roles:
• Anonymous user — readers of the site who either do not have an account or
are not logged in.
• Authenticated user — All non-anonymous users inherit the "authenticated user
role."
• Administrator - This role has all permissions enabled by default.
implementation_status: In Place
- key: d



components/Drupal/AC- | hyperGRC - Reusable Comp | tools/secrender/secrend | ComplianceAsCode/drup

GitHub, Inc. (US) https://github.com/ComplianceAsCode/drupal 110%

Most Visited | Fen | DevOps | Devel | CivicActions | Cool | News | PGH | Stevo | Etc. | Lenovo | Imagine | OpenPrivacy | Imported

Drupal Projects Compliance Controls

This repository contains compliance information for various Drupal projects commonly used to harden a Drupal instance to meet various NIST SP 800-53 described security controls.

This data adheres to the OpenControl schema for building compliance documentation and can be used to support your own authority to operate (ATO) review process. The documentation generated from this content can be used to assist your organization in authorizing Drupal. For more information, visit http://open-control.org.

> This content is provided for informational purposes only and has not been vetted by any third-party security assessors. You are solely responsible for developing, implementing, and managing your applications and/or subscriptions running on your own platform in compliance with applicable laws, regulations, and contractual obligations. The documentation is provided "as-is" and without any warranty of any kind, whether express, implied or statutory, and Docker, Inc. expressly disclaims all warranties for non-infringement, merchantability or fitness for a particular purpose.

Summary of projects and related controls

Drupal Project	800-53 Control
Automated Logout	AC-12 Session Termination

CivicActions

components/Drupal/AC- | hyperGRC - Reusable Comp | tools/secrender/secrend | ComplianceAsCode/drup

GitHub, Inc. (US) https://github.com/ComplianceAsCode/drupal

Most Visited | Fen | DevOps | Devel | CivicActions | Cool | News | PGH | Stevo | Etc. | Lenovo | Imagine | OpenPrivacy | Imported

Drupal Project	800-53 Control
Automated Logout	AC-12 Session Termination
Ejector Seat	AC-12 Session Termination
Flood-control	SC-5 Denial Of Service Protection
GovReady	AC-2 (f) Account Management; MA-1 System Maintenance Policy and Procedures; MA-2 Controlled Maintenance;
Password Policy	AC-3 Access Enforcement
Paranoia	AC-6(1) Least Privilege - Authorize Access To Security Functions
Security Kit	SC-4 Information in Shared Resources; SC-8 Transmission Confidentiality and Integrity; SC-11 Trusted Path; SC-23 Session Authenticity;
Security Review	AC-4 Information Flow Enforcement; AC-6 Least Privilege; CM-6 Configuration Settings; CM-7 Least Functionality)
Session Limit	AC-12 Session Termination
TFA	AC-2 Account Management; AC-6 Least Privilege;
Watchdog / dblog	AU-2 Audit Events; AU-3 Content Of Audit Records; AU-7 Audit Reduction And Report Generation; AU-8 Time Stamps; AU-9 Protection Of Audit Information; AU-14 Session Audit;

components/Drupal/AC- | hyperGRC - Reusable Compl | tools/secrender/secrend | ComplianceAsCode/drup

GitHub, Inc. (US) https://github.com/ComplianceAsCode/drupal 110%

Most Visited Fen DevOps Devel CivicActions Cool News PGH Stevo Etc. Lenovo Imagine OpenPrivacy Imported

How to use

Docs with generated and paste text

The `docs/` directory contains generated documents from which you can copy text.

- BASIC.md - A basic listing of controls supported by Drupal projects tracked in this repository

Scripts to generate documents

The `scripts/` directory contains ready-to-run python scripts to generate various documents from Jinja2 templates in the `scripts/templates/` directory.

Using in OpenControl files

You can include this repository as a dependency by adding the appropriate lines from the below snippet to your `opencontrol.yaml` file:

```
dependencies:
  systems:
    - url: https://github.com/opencontrol/Drupal-Projects-Compliance-Controls
      revision: master
```

Automate the System Security Plan (SSP) creation

1. Sharing of control information
2. Reusable components
3. Machine readable OpenControl YAML files in git
4. Automated document creation
5. Automated evidence collection and control verification

NIST SP 800-53 Revision 4

AC: Access Control

AC-1: Access Control Policy And Procedures

> The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].

AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Providers dated 1 May 2013.

CivicActions

CivicActions has developed, documented and disseminated to personnel an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls. This information is maintained in the CivicActions Access Control (AC) Policy. This document can be found in the CivicActions Compliance Docs GitHub repository at https://github.com/CivicActions/compliance-docs

Reusable Component Library System Security Plan

NIST SP 800-53 Revision 4

AC: Access Control

AC-1: Access Control Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].

AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Providers dated 1 May 2013.

CivicActions

CivicActions has developed, documented and disseminated to personnel an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls. This information is maintained in the CivicActions Access Control (AC) Policy. This document can be found in the CivicActions Compliance Docs GitHub repository at https://github.com/CivicActions/compliance-docs.

AC-2: Account Management

The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. 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; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: AWS account management.

a

AWS

AWS Identity and Access Management (IAM) provides fine-grained access to AWS resources Operations, in collaboration with the Security Office, will set up privileged accounts accounts for the following roles: • Reporter - account that has read-only access to system reporting. • Administrator - account with full site management access.

Drupal

Drupal provides user accounts for individuals who participate in visiting, contributing to and administering the site with the following roles: • Anonymous user – readers of the site who either do not have an account or are not logged in. • Authenticated user – All non-anonymous users inherit the "authenticated user role." • Administrator - This role has all permissions enabled by default.

SSH

Operations, in collaboration with the Security Office, will set up privileged accounts accounts for the following roles: • Developer - user level account that has access to application features and sanitized databases • System Administrator - user accounts that enjoy full system administrator (sudo) access

b

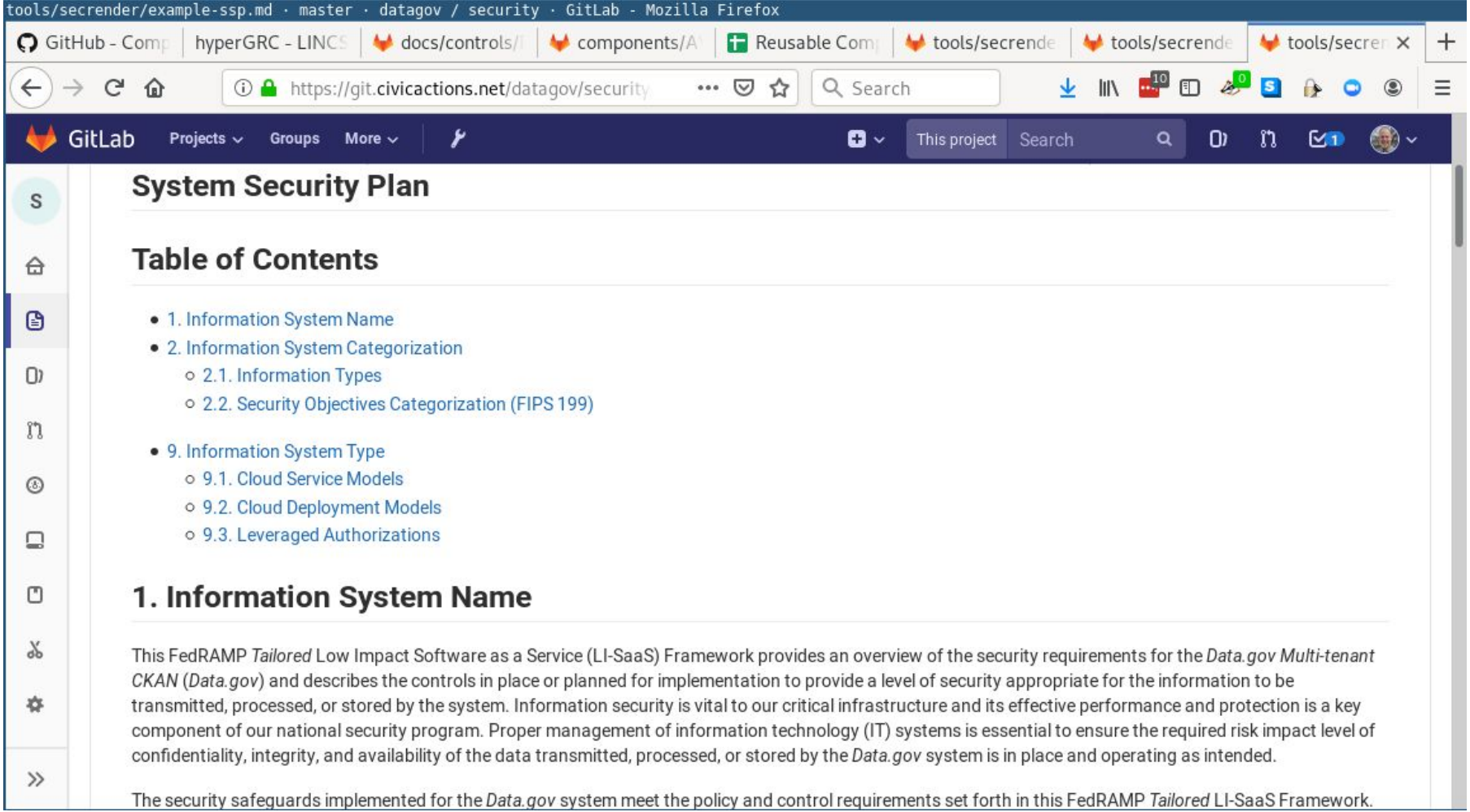
CivicActions

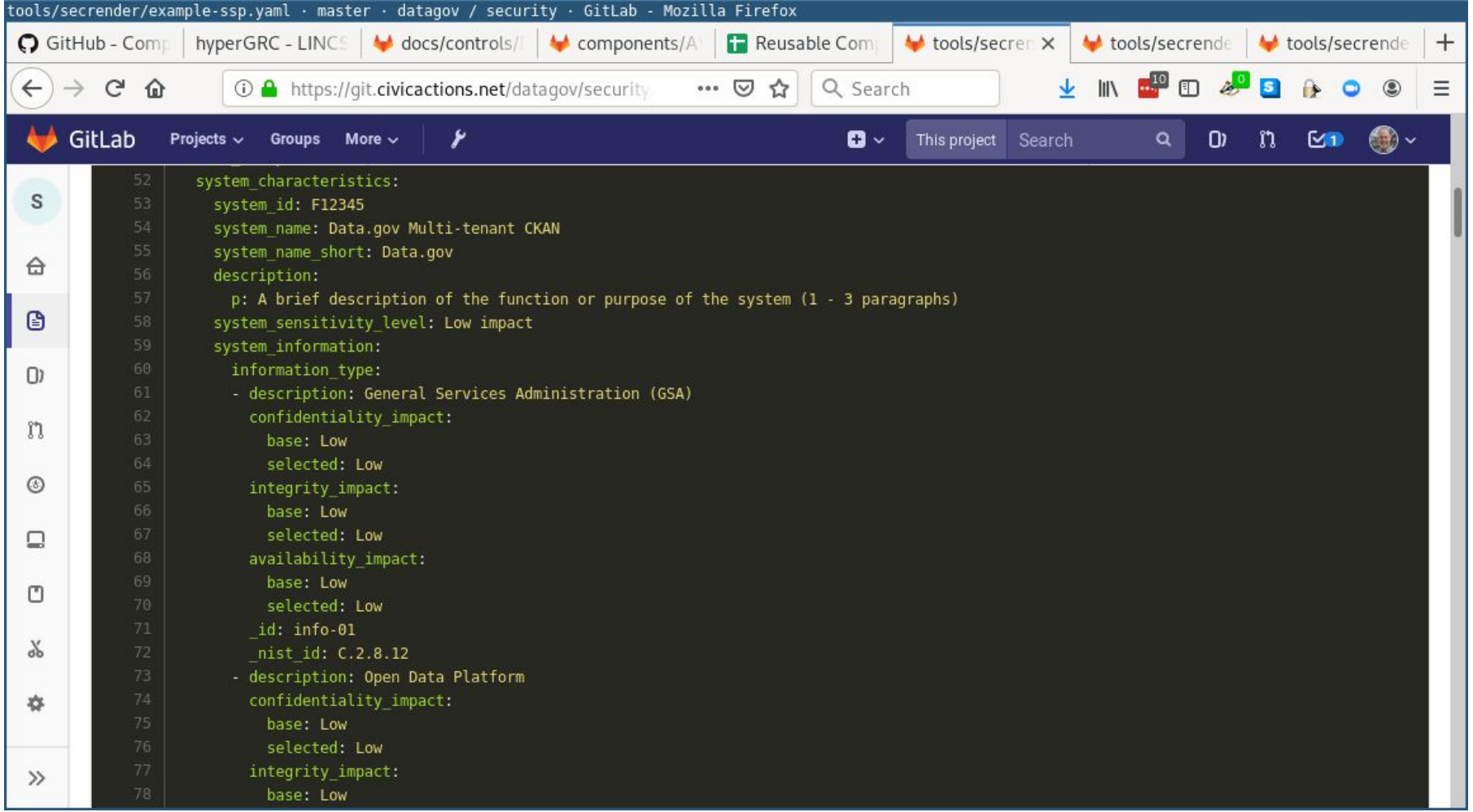
CivicActions' Project Manager assigns the "admininstrator" role for the management of all accounts issued to internal admin roles supporting the information system. Account requests are initiated by the Project Manager by completing a ticket request and the CivicActions Operation Team manages the entire account creation process.

d

CivicActions

All accounts issued for application administrators and SSH are documented in CivicActions' ticketing system. Account request tickets contain details that explain the attributes for the account including authorized users of Drupal, system infrastructure, group and role membership, and access authorizations.


GitHub - Comp
hyperGRC - LINCS
docs/controls/I
components/A
Reusable Com
tools/secrende
tools/secrende
tools/secren
https://git.civicactions.net/datagov/security
Search
GitLab
Projects
Groups
More
This project
Search
System Security Plan
Table of Contents
1. Information System Name
2. Information System Categorization
2.1. Information Types
2.2. Security Objectives Categorization (FIPS 199)
9. Information System Type
9.1. Cloud Service Models
9.2. Cloud Deployment Models
9.3. Leveraged Authorizations
1. Information System Name
This FedRAMP Tailored Low Impact Software as a Service (LI-SaaS) Framework provides an overview of the security requirements for the Data.gov Multi-tenant CKAN (Data.gov) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology (IT) systems is essential to ensure the required risk impact level of confidentiality, integrity, and availability of the data transmitted, processed, or stored by the Data.gov system is in place and operating as intended.
The security safeguards implemented for the Data.gov system meet the policy and control requirements set forth in this FedRAMP Tailored LI-SaaS Framework.



CivicActions

tools/secrender/example-ssp.md.j2 · master · datagov / security · GitLab - Mozilla Firefox

GitHub - Comp | hyperGRC - LINCS | docs/controls/I | components/A | Reusable Com | tools/secrende | tools/secrer | tools/secrende

https://git.civicactions.net/datagov/security

Search

GitLab Projects Groups More This project Search

```
Table 2-2. Information Type

<table>
<thead>
<tr class="header">
<th><p>Information Type</p>
<p>(Use only information types from NIST SP 800-60, Volumes I and II as amended)</p></th>
<th>NIST 800-60 identifier for Associated Information Type</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
{%- for info_type in ssp.system_characteristics.system_information.information_type %}
<tr class="odd">
<td>{{ info_type.description }}</td>
<td>{{ info_type._nist_id }}</td>
<td>{{ info_type.confidentiality_impact.selected }}</td>
<td>{{ info_type.integrity_impact.selected }}</td>
<td>{{ info_type.availability_impact.selected }}</td>
</tr>{% endfor %}
</tbody>
</table>

## 2.2. Security Objectives Categorization (FIPS 199)
```

CivicActions

2.1. Information Types

This section describes how the information types used by *Data.gov* are categorized for confidentiality, integrity, and availability of sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from *Data.gov*. The selection of the information types is based on guidance provided by the Office of Management and Budget (OMB) Federal Enterprise Architecture (EA) Program Management Office (PMO) Business Reference Model 2.0, National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST Special Publication 800-60 (NIST SP 800-60) , *Guide for Mapping Types of Information and Information Systems to Security Categories*.

FIPS 199[1] allows for a full range of information types. In order to meet specific, niche needs of systems, Agencies can specify the types of information being placed in the cloud environment. For FedRAMP *Tailored* LI-SaaS, Agencies can specify the type(s) of information that will reside in FedRAMP *Tailored* LI-SaaS applications/systems.

Table 2-2. Information Type

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability
General Services Administration (GSA)	C.2.8.12	Low	Low	Low
Open Data Platform	C.3.5.9	Low	Low	Low

components/Drupal/AC- | hyperGRC - Reusable Comp | tools/secrender/secrend

https://git.civicactions.net/datagov/security/blob/master/tools/secren 120%

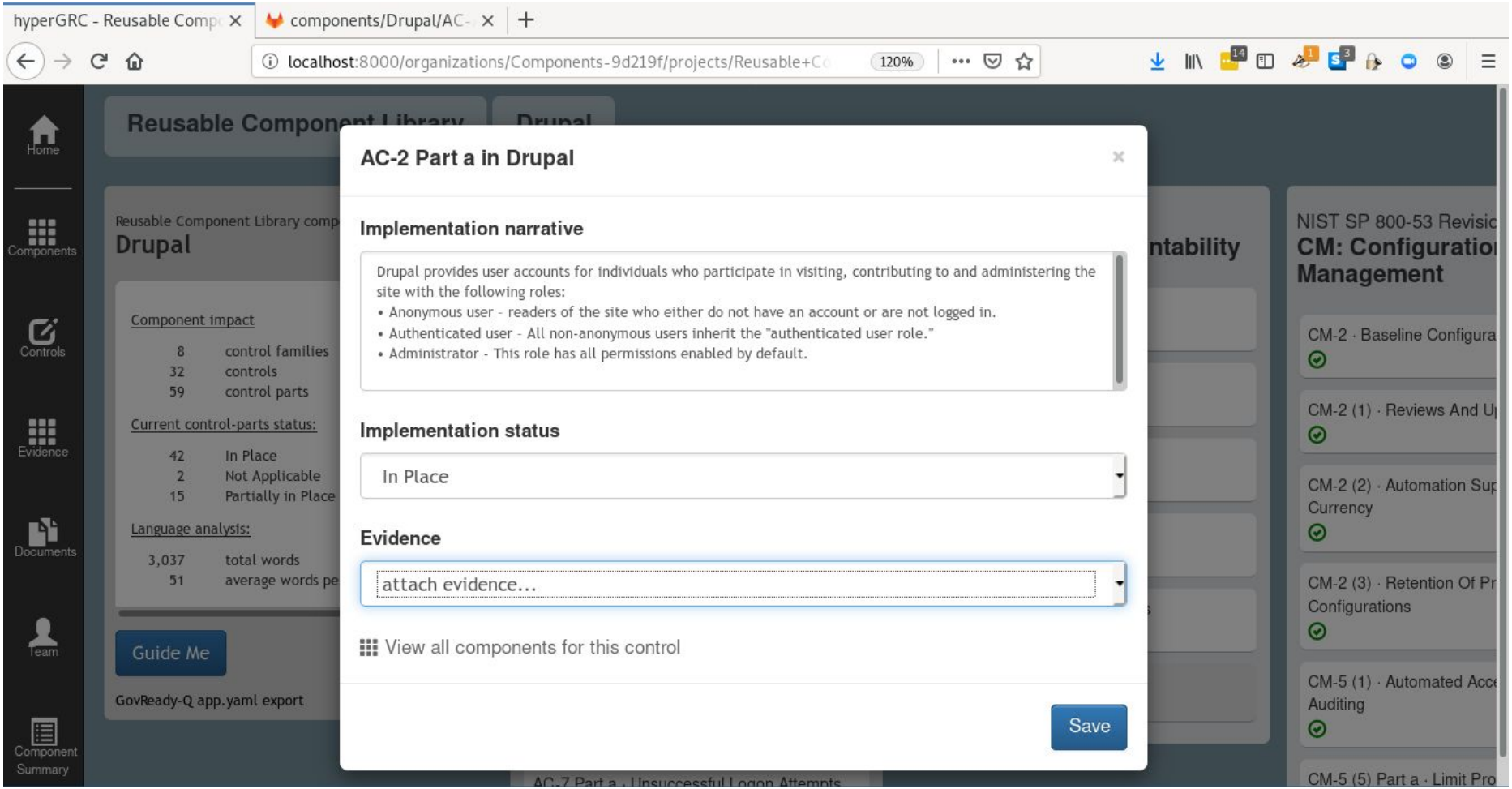
Most Visited | Fen | DevOps | Devel | CivicActions | Cool | News | PGH | Stevo | Etc. | Lenovo | Imagine | OpenPrivacy | Imported

GitLab Projects Groups More This project Search

```
34  def main(in_, template_path, root):
35      with open(in_, "r") as stream:
36          yaml = load(stream, Loader=FullLoader)
37
38      template = get_template(template_path)
39
40      template_args = dict()
41      template_key, yaml_key = root.split(':')
42
43      if yaml_key not in yaml:
44          raise click.ClickException('Key {0} not found in input values'.format(yaml_key))
45
46      template_args[template_key] = yaml[yaml_key]
47      output = template.render(**template_args)
48
49      print(output)
50
51  def get_template(template_path):
52      abs_path = os.path.abspath(template_path)
53      template_dir, template_file = os.path.split(abs_path)
54      templateLoader = jinja2.FileSystemLoader(searchpath=template_dir)
55      templateEnv = jinja2.Environment(loader=templateLoader)
56      template = templateEnv.get_template(template_file)
57
58      return template
```

Automate the System Security Plan (SSP) creation

1. Sharing of control information
2. Reusable components
3. Machine readable OpenControl YAML files in git
4. Automated document creation
5. Automated evidence collection and control verification



CivicActions

components/Drupal/AC- | hyperGRC - Reusable Comp | tools/secrender/secrend | Chef InSpec | Chef | inspec/inspec: InSpec: Au

GitHub, Inc. (US) | https://github.com/inspec/inspec

Most Visited | Fen | DevOps | Devel | CivicActions | Cool | News | PGH | Stevo | Etc. | Lenovo | Imagine | OpenPrivacy | Imported

README.md

Chef InSpec: Inspect Your Infrastructure

- **Project State: Active**
- **Issues Response SLA: 3 business days**
- **Pull Request Response SLA: 3 business days**

For more information on project states and SLAs, see this documentation.

slack 210/6886 | build passing | master - Ok | coverage 84%

Chef InSpec is an open-source testing framework for infrastructure with a human- and machine-readable language for specifying compliance, security and policy requirements.

```
# Disallow insecure protocols by testing

describe package('telnetd') do
  it { should_not be_installed }
end

describe inetd_conf do
  its("telnet") { should eq nil }
end
```

CivicActions

A Culture of Security

It's cool to be secure

CivicActions

A Culture of Security

- ➔ Require use of a Password Manager
  - ➔ Recommend use for personal accounts, too
- ➔ Require 2FA for Privileged Accounts
  - ➔ Including email, password manager, banks, ...
- ➔ Give everyone a Yubikey
  - ➔ Ensure 2FA accounts have redundancy
- ➔ Phishing expeditions can be Phun!
  - ➔ Support the team in catching phish

A Culture of Security

- Require use of a Password Manager
  - Recommend use for personal accounts, too
- **Require 2FA for Privileged Accounts**
  - **Including email, password manager, banks, ...**
- Give everyone a Yubikey
  - Ensure 2FA accounts have redundancy
- Phishing expeditions can be Phun!
  - Support the team in catching phish

A Culture of Security

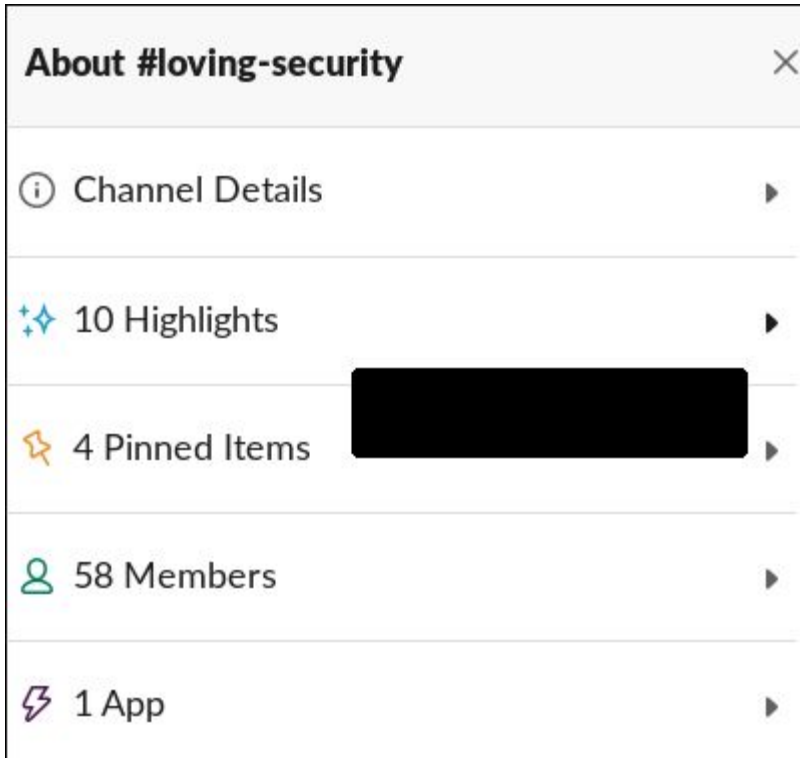
- Require use of a Password Manager
  - Recommend use for personal accounts, too
- Require 2FA for Privileged Accounts
  - Including email, password manager, banks, ...
- **Give everyone a Yubikey**
  - **Ensure 2FA accounts have redundancy**
- Phishing expeditions can be Phun!
  - Support the team in catching phish

A Culture of Security

- Require use of a Password Manager
  - Recommend use for personal accounts, too
- Require 2FA for Privileged Accounts
  - Including email, password manager, banks, ...
- Give everyone a Yubikey
  - Ensure 2FA accounts have redundancy
- **Phishing expeditions can be Phun!**
  - **Support the team in catching phish**

#loving-security

Optional slack channel with 74% subscription rate



DEMANDS

CivicActions

Next Steps

There's opportunity for making compliance secure

CivicActions

Next Steps

- ➔ Publishing reusable components
- ➔ Evidence collection and verification
- ➔ Building SSPs in the CI pipeline
- ➔ NIST OSCAL
- ➔ FISMAtic
- ➔ GovReady-Q
- ➔ Public CM APIs and data formats

Next Steps

- Publishing reusable components
- **Evidence collection and verification**
- Building SSPs in the CI pipeline
- NIST OSCAL
- FISMAtic
- GovReady-Q
- Public CM APIs and data formats

Next Steps

- ➔ Publishing reusable components
- ➔ Evidence collection and verification
- ➔ **Building SSPs in the CI pipeline**
- ➔ NIST OSCAL
- ➔ FISMAtic
- ➔ GovReady-Q
- ➔ Public CM APIs and data formats

Next Steps

- ➔ Publishing reusable components
- ➔ Evidence collection and verification
- ➔ Building SSPs in the CI pipeline
- ➔ **NIST OSCAL**
- ➔ FISMAtic
- ➔ GovReady-Q
- ➔ Public CM APIs and data formats

Next Steps

- ➔ Publishing reusable components
- ➔ Evidence collection and verification
- ➔ Building SSPs in the CI pipeline
- ➔ NIST OSCAL
- ➔ **FISMAtic**
- ➔ GovReady-Q
- ➔ Public CM APIs and data formats

Next Steps

- ➔ Publishing reusable components
- ➔ Evidence collection and verification
- ➔ Building SSPs in the CI pipeline
- ➔ NIST OSCAL
- ➔ FISMAtic
- ➔ **GovReady-Q**
- ➔ Public CM APIs and data formats

Next Steps

- ➔ Publishing reusable components
- ➔ Evidence collection and verification
- ➔ Building SSPs in the CI pipeline
- ➔ NIST OSCAL
- ➔ FISMAtic
- ➔ GovReady-Q
- ➔ **Public CM APIs and data formats**

https://www.agilegovleaders.org

agl

Agile Government Leadership

Search ...

About Blog AGL Live Resources Events Get Involved Log In

Agile Government Leadership

A nonprofit association helping government modernize

Subscribe

Learn

Join

More info...

Some links from this talk

- https://civicactions.com
- https://github.com/CivicActions
- https://github.com/opencontrol
- https://github.com/usnistgov/OSCAL
- https://github.com/GovReady/hyperGRC
- https://github.com/uscensusbureau/fismatic
- https://github.com/ComplianceAsCode/drupal
- https://nvd.nist.gov/800-53/Rev4
- https://www.agilegovleaders.org

Thank You.

Fen Labalme, CISSP
fen@civicactions.com
@openprivacy