CMS and What Makes an Agency Ready for Security Automation with OSCAL?

A Vendor’s View

Presented by:
Greg Elin, Compliance as Code Enthusiast
Just Stepping In...

Experienced Vendor & Ex Federal Employee

- Presentational substitute for Andrés Colón, Senior Technical Analyst, Office of Information Technology, EADG / TEA, CMS
- Not representing CMS
- Speaking as a vendor in the Compliance as Code space
- Not selling anything

Brief Bio
Greg Elin, CEO, CAC Vendor
- Former Chief Data Officer at FCC (GS-15)
- Multiple agencies exploring Compliance as Code
- Avid member of the Compliance as Code community
Introduction

Part of U.S. Department of Health and Human Services (HHS).
Over 200 SSP’s within the agency.
Lots of organization information online.

Large ATO Improvement Project

CMS pursuing a large effort to improve ATO process.
Multiple projects, teams, and vendors
Part of CMS’s BlueSky Initiative.
The BlueSky Initiative was conceived to conceptualize and capture what an ideal and effective security process would encompass to benefit people, build secure systems and minimize the risk to CMS’s mission. Rapid ATO is one of the projects coming out of the Blue Sky Security Initiative at CMS.
Concrete Next Steps

In the 12 months we are focusing on:

1. Incorporate human centered design and agile best practices throughout the modernization lifecycle
2. Begin demystifying the authorization event for product teams
3. Reduce the burden in writing control compliance descriptions
4. Pilot initiatives to guide teams through authorization
5. Pilot tools to help developer build more secure software
6. Map business processes and identify opportunities for improvements, designing with our users solutions that actually meet their needs
7. Promote cross-functional collaboration of leaders of emerging best practices
What CMS had Accomplished So Far

**Procurement**
- Established OIT Security Pilot. Identified over 1500+ high security vulnerabilities in public CMS open source software.
- Rapid ATO Procurement.
- TEA worked with OAGM and ISPG to establish a procurement strategy to make incremental progress on the tactical next steps discussed in this presentation. Contract started on 9/30/2020.

**Community Engagement**
- Created the Compliance as Code Workgroup.
- Engaged CMS Business Units, NIST, USDS, DHS, US Navy and others for security cross-pollination initiatives.
- Participating in the On-going Authorization Workgroup.
- Established the CMS Slack Chat #security_community. 70+ security experts from CMS.

**Skill Building**
- Trained teams on how to perform automated system composition analysis to identify vulnerabilities with the Snyk Pilot.
- Helped organize brown bags on security best practices.
Opportunity

Standardized, reusable templates will greatly simplify SSP creation.

- “To give people that TurboTax experience, you need a library of pre-written control content for all of the different components that people would commonly use.”
- “You’re going to want to make as much of that [security documentation] reusable as possible, so one of my goals has been to make templates and make them as generic as possible”
- “If you know that you have a similar SSP, you can grab that as a template to start with.”
Projects with Vendors

- **Adopting OSCAL**
  
  Analyzing existing corpus of SSP’s using NLP (Natural Language Processing) and participating in OSCAL community.

- **Creating an Initial Library of “Certified Control Sets”**
  
  Commitment to create large enough sample library of components to viably test reuse and automation.

- **Automated Evidence Gathering**
  
  Provided evidence and compliance as a service so ADO (Application Development Organization) gets evidence early in SDLC (System Development Life Cycle).
Certified Sets

What is a “Certified Set”? 
A set of technologies that have been pre-approved / vetted and can be reused. Includes language, sample implementation, plain language, and attestation.

Why it Matters? 
Providing certified Sets provides business owners with a standard that increases the potential for re-use, automation and collaboration.

Think of a Certified Set as pre-approved building plan

Slide Courtesy of CMS
Agency Readiness for CAC

01 Sharing Culture
The culture at CMS mirrors the spirit of compliance as code. Information is shared online and publicly. Access to resources is a cultural norm.

02 Active Teams
Teams are motivated and involved in the creation of policies.

03 Expertise (CAC and Tools)
CMS teams are experienced in git repositories, collaborative spaces, and vendor chats. Expertise in these areas impacts compliance as code thinking in organizations.

04 Champions
The executive level at CMS is engaged in the CAC project. CMS leaders regularly attend presentations as well as regular meetings. The project leads are similarly empowered and enthusiastic by CAC.
Centers for Medicaid and Medicare Services shares the complete Information Security and Privacy Library on CMS.gov. The site provides a comprehensive listing of policy guidance, standards, regulations, laws, and other documentation related to the CMS Information Security and Privacy Program.
Who CMS collaborates with
Major Parties involved in Compliance

- **Product Team Independent Assessor**
  - Implement and document system implementation

- **Authorizing Official**
  - Review system documentation and implementation, create assessment

- **System Security Officer**
  - Review security assessment, grant ATO

**Information System Security Officer**
- Manages System Security and Risks

*Slide Courtesy of CMS*
Sample Vendor Partners & Projects

- GovReady
- CivicActions
- MITRE
- CaaS
- NIST
- Ad Hoc
- Others
Any agency looking to create a compliance as code initiative needs to be aware of the mindsets and resources that are needed for an implementation of CAC to be successful and impactful for an organization.

### Ideal
Paradigms and Processes for Success

- Vision
- Concrete Steps
- CAC Experience
- IT Committed to Removing Pain
- Budget
- Examples:
  - CMS, USDA

### Challenging
Pitfalls and Obstacles

- “Just Looking”
- Vague direction
- Try one or two systems
- Little or no budget
Federal Agency and **OSCAL**

**Vendor’s Perspective**

**Essential**
- Executive Buy-in
- Champions
- Funding
- Access to Some Content
- Shared Developer Environment
- Access to Existing GRC Tools

**Better**
- Vision
- Community Engagement
- Access to Lots of Content
- Easy-to-Use Developer Environment
- Compliance as Code Experience
- Time

**Best**
- Executive Participation
- Human-Centered Design
- Active User Testing
- IT Wanting to Relieve Pain
- Not Vendor Driven
- Incremental Value
Contact

Andrés Colón
Senior Technical Analyst
Office of Information Technology
EADG / TEA
andres.colon@cms.hhs.gov

Rajiv Uppal
Chief Information Officer

Nicholas Wojnowski
Program Officer / PMP / SME

Gus Borjas
Cyber Risk Advisor / SME

Why this Matters
Support with Transformation
Incremental Value

Slide Courtesy of CMS