OSCAL Developer Data Bites

April 4, 2024

info@fedramp.gov

fedramp.gov

Purpose: To create space for dialogue between developers who use OSCAL and the FedRAMP® automation team.

Outcomes:

- Shared understanding of the projected roadmap for the FedRAMP program
- Shared understanding of how OSCAL and automation fit into upcoming milestones for the PMO
- Productive discussion around OSCAL

Agenda:

- Welcome
- General Updates
- Pre-Submitted Q&A
- FedRAMP Program Roadmap Updates
- Open Forum
- Next Steps & Closing

Data Bites Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

General Updates

FedRAMP Automation Community Updates

Revising OSCAL Guides

FedRAMP automation team is continuing to work towards publishing HTML versions of the OSCAL guides to replace the current PDF versions.

- Newer version of Hugo USWDS theme (PR#581)
- Restructuring of content to provide better integration of general vs model-specific guide content (PR#581)
- Reviewing all FedRAMP OSCAL validation rules and constraints to ensure they are accurately documented in the guides, with examples when applicable
- Diagrams as Code - starting to evaluate use of PlantUML for OSCAL model diagrams in documentation
- Working with internal FedRAMP documentation teams to establish clearer guidelines for printables / documents generated from source OSCAL (e.g., SSP)

Local Validation Tooling

- FedRAMP automation team is working on adding metaschema validation mechanisms in the OSCAL-CLI tool

GitHub Issues & PRs

- 11 new issues opened

- 3 closed issues

- Merged 4 PRs

- 7 other proposed PRs

Items of Note

- Merged issue #533 which Updated FedRAMP baselines based on NIST SP 800-53 rev5.1.1 release

- PR #581 - Theme and organizational improvements for markdown guides

- View the project workboard for more details on ongoing work and upcoming priorities

Pre-Submitted Questions

None received!

Reminder to submit questions/topic ideas via **https://forms.gle/M4pT7P2xyE6hRC7DA**

FedRAMP Program Roadmap Update

We are making a roadmap to:

- Respond to stakeholder feedback that the program's growth is not enough to **meet the needs of the market.**
- Clearly define **GSA's and FedRAMP's strategic goals**, and make sure the program's resources are prioritized around them.
- Communicate publicly that **FedRAMP is committed to modernizing**, with enough key details to show how and why.

[Read our blog post to learn more about FedRAMP's Roadmap and why it matters](#)

200+

Federal Agencies

400+

Cloud Service Providers (CSPs)

* Including 60+ small businesses

40+

Third Party Assessment Organizations (3PAOs)

Our Commitment to Our Customers

FedRAMP will **make it safe and easy** for the U.S. government to **take full advantage of cloud services** to meet its mission.

We are driving towards a future with...

Improved Customer Experience

- Growth of a trusted marketplace of cloud services available for federal agencies

- Engagement with a larger, more technical PMO staff

Stronger Security and Risk Management

- Increased visibility into the security posture of CSPs through centralized continuous monitoring

- More clear and consistent security expectations with supporting guidance

Reduced Time and Cost

- Less manual and time intensive to create and share authorization packages

- Reduced time and cost to review and assess authorization packages

- Reduced manual effort and time to complete continuous monitoring

Strategic Goals - Our Focus for 2024-2025

1 Orient FedRAMP around the **customer experience.**

2 Position the program as a **leader in cybersecurity** and risk management.

3 Significantly **scale** the size and scope of a **trusted FedRAMP marketplace.**

4 Increase **program effectiveness** through automation and technology-forward operations.

1

Orient FedRAMP around the customer experience

Challenge

Cloud service providers have found it difficult to navigate a process that takes too long and costs too much to achieve a FedRAMP authorization and implement new features.

What We Will Deliver First

- **Enable agile software delivery** by piloting a replacement "significant change request" process that does not block on advance approval.

- **Tackle known key policy obstacles** that inhibit larger security goals in the authorization process (e.g., cryptography requirements, how cloud providers integrate with other cloud providers).

- **Increase clarity on how to successfully navigate FedRAMP** by creating a living knowledge base of guidance, training, and real-world examples.

- **Incentivize CSPs to provide secure configuration profiles** and guidance on the use of their services, in collaboration with CISA.

2

Position the program as a leader in cybersecurity and risk management

Challenge

FedRAMP is a security and risk management program and people expect that authorized services meet a certain security bar.

What We Will Deliver First

- **Bring more technical capacity and expertise** into the FedRAMP program (at GSA) and ecosystem (agency partners).

- **Define the core security expectations** for all FedRAMP authorizations in support of a government-wide presumption of adequacy.

- **Define initial approach for reciprocity between FedRAMP and external frameworks**, starting with low-impact SaaS.

3

Significantly scale the size and scope of a trusted FedRAMP marketplace

Challenge

Despite its growth over the years, the FedRAMP marketplace has not kept pace with agency demand for new and innovative services.

What We Will Deliver First

- **Implement low-review process with trusted authorizing partners.** Pursuing a pilot with the Department of Defense.

- **Form initial joint authorization groups** to reduce extra reviews and delays in FedRAMP authorization.

- **Centralize and automate continuous monitoring** to reduce burden and improve visibility into the cybersecurity posture of cloud service providers.

4

Increase program effectiveness through automation and technology-forward operations

Challenge

FedRAMP processes are too manual and take too long, and its performance metrics should drive program outcomes that more fully address customer needs.

What We Will Deliver First

- **Publish new key performance metrics aligned with the lived customer experience**, including their time and cost outcomes.

- **Establish a new FedRAMP technology platform** that will facilitate a data-first, api-first foundation for agencies and cloud providers to send and receive security information from FedRAMP.

- **Support machine-readable "digital authorization packages"** to support automation. Piloting with commercial cloud providers, and agency partners.

Benefits We Will Deliver to Our Customers

Cloud Service Providers

- Can see how to deploy significant changes without blocking on federal approval

- Can use and contribute to a growing public knowledge base

- **Can confidently build, validate and submit a digital authorization package**

- Are seeing the program's metrics reflect their own experience

Authorization Teams (Agencies and PMO)

- All authorizers should have a platform that eases the authorization and review process

- **Pilot partners should see reduced PMO review of their packages based on their mature processes**

- **Are led and engaged by a larger, more technical PMO staff**

Agencies

- Have a centralized repository that accommodates all authorization packages

- **Have the tools to review digital authorization packages**

Help Shape FedRAMP's Future

FR ™

Participate in a partnership or pilot

A number of items in this roadmap will require pilots with different stakeholders - let FedRAMP know if you are interested in participating.

Provide public comment on future guidance

We will be doing frequent public comments - major items that impact our stakeholders will have public comment periods.

Engage in upcoming public forums

Join us on Thursday, April 11 for the first public forum on the FedRAMP Roadmap.

Open Forum

Thank you

Our next Developer Data Bites virtual meeting will be on

Thursday, May 2, 2024 at 12p ET.

Submit questions and future discussion topics to OSCAL@fedramp.gov

Learn more at fedramp.gov

@FEDRAMP