April 14, 2025
fedramp.gov/20x

FedRAMP20X

REV5 Continuous Monitoring Working Group Kick-Off

Starting at 1:03pm

[REC ●]

Today's Agenda

- Recap of How We Will Work
- Discussion Forum Analysis
- FedRAMP Horizons
  - SCR Updated Standards
  - Continuous Monitoring Scorecard
  - FedRAMP Repo Standards
- Next steps

Goals for today

Recap how this working group will operate

Discussion Forum Analysis

Discuss standards in development or on the horizon for Rev5

How we'll work

The purpose of bi-weekly meetings is to recap discussions taking place in GitHub

For all of our Working Groups:

The Working Group GitHub Repo will be the source of work/truth. This includes:

- All discussions related to the working group
- Development/demonstration of proof of concepts
- Providing a venue for information sharing that may inform updates in standards
- Development of next working group's agenda
- Meeting minutes and recording
- This is a part of our commitment to operating in public, transparently, in a way that fosters collaboration amongst the variety of stakeholders

Thank you for your participation so far!

- 15 individual discussions
- 129 top level comments
- 200 comment replies
- 91 unique users

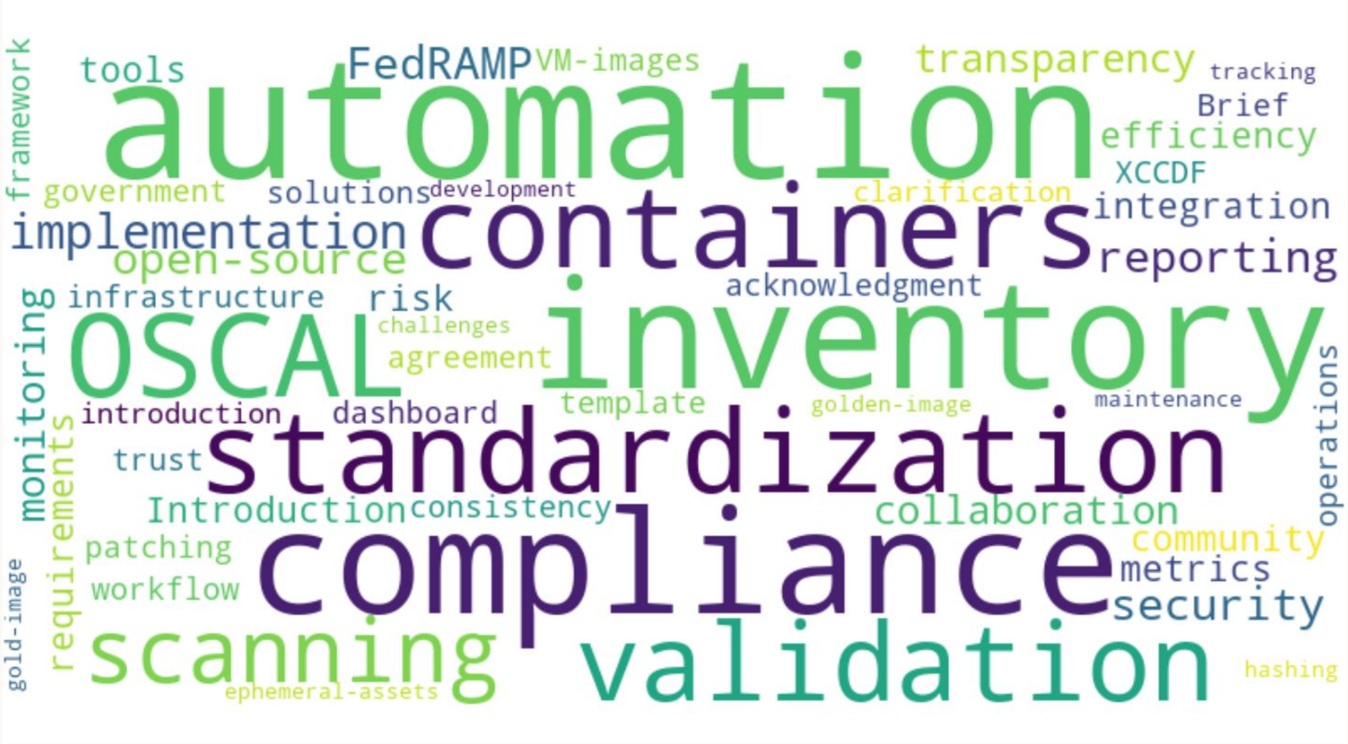
Top Individual Contributors:

- cybersechawk
- sunstonesecure-robert
- atfurman
- Bscudera9
- kamamanh
- JosephScarzone
- trumant
- Telos-sa
- austinsonger

Discussion Keywords

Top Five Keywords:

1. Automation
2. Inventory
3. Compliance
4. Containers
5. Standardization



Thoughts on current SCR Process

…a "black hole" where there's unclear ownership of review responsibilities, as agencies typically focus only on their specific applications rather than the underlying infrastructure…

…legacy, cumbersome, and often becomes a bottleneck in service delivery…

…formerly JAB systems are required to complete a Security Assessment Report (SAR) for every SCR, while Agency authorizations allow for assessing changes during annual reviews…

…challenges for Infrastructure as a Service (IaaS) providers, noting that authorizing agencies typically focus on applications running on the IaaS rather than the infrastructure itself…

…multiple layers of approval for changes that may not warrant such scrutiny, excessive control testing requirements that don't add meaningful value, and delays in implementing important updates due to the lengthy approval process…

Suggestions for improvements to SCR Process

…shift away from the current rigid SCR process toward a more flexible, risk-based approach that empowers Cloud Service Providers (CSPs) to manage changes through their internal control mechanisms…

…recommend implementing API-driven evidence collection, standardized Key Security Indicators (KSIs) across control domains, and automated SCR approval pipelines…

… improve the process by making it more transparent and collaborative, for example, releasing draft templates and documentation for public review and feedback…

…allow CSPs to conduct internal testing of changes, implement them, and have the Third Party Assessment Organizations (3PAOs) evaluate these changes during annual assessments…

…if a CSP can demonstrate effective change management processes, they should be trusted to implement changes without requiring separate approval for each significant change…

Simplifying SCRs

- The FedRAMP PMO is actively working on a new SCR Standard Process
  - Previous guidance dates back to 2018 and relies on overly manual processes
  - Builds upon our Agile Delivery Pilot from 2024
  - Sets parameters for notification vs approval requirements
  - Prioritizes security and adaptability over a monolithic tiered oversight model
  - Rewards secure by design principles
- We will leverage feedback in the form of best practices, lessons learned, and general feedback from the GitHub discussion forums to inform drafts
- All FedRAMP policy will undergo a public Request For Comment period, which is when everyone will get their opportunity to provide direct input.

Developing a Continuous Monitoring Scorecard

- The intent is to shift continuous monitoring activities away from delivering paperwork to an activity that better informs agencies of the overall CSP posture
- This will NOT change your systems continuous monitoring requirements but changes some of the “how”
- This should reduce the burden of transforming outputs to meet FedRAMP templates
- Reduces the burden of duplication of files across internal/external repos (more on MAX transition later)
- We will leverage feedback in the form of best practices, lessons learned, and general feedback from the GitHub discussion forums to inform drafts
- We will pilot this effort prior to drafting any formal standards and will solicit volunteers CSPs/Agencies within GitHub

FedRAMP Package Repo Standards

- FedRAMP will establish a formal standard for CSPs to facilitate secure storage, access, and transmission to FedRAMP authorization data
- As a standard is published, FedRAMP managed MAX/Connect.gov services will sunset over the next 1-2 years
  - This should only affect LOW/MOD packages
  - HIGH packages have always been managed by CSPs in conjunction with Agency partners
- If current managed repositories exists CSPs may opt-in to transition

Working Group Next Steps

- Our next recap will be held on **28 April at 1 PM EST.**

- If you are interested in bringing forward a topic to this working group, post in the discussion forums
  - **<u>This is NOT an opportunity for product pitches</u>**

Close-out