May, 2025

fedramp.gov/20x

FedRAMP20X

Automating Assessment Working Group Townhall

Starting at 1:03pm until 1:30 pm


[REC ●]

Today's Agenda

- GitHub Discussion Recap
- Pilot Deliverables Recap
- Draft Pilot Submissions
- Final Pilot Submissions
- Discussion Starters
- Next Steps

Workgroup Discussion Forum on GitHub:

https://github.com/FedRAMP/automating-assessment-cwg/discussions

Workgroup Video Recordings:

https://www.youtube.com/@FedRAMP/videos

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 guidance
- This is a part of our commitment to operating in public, transparently, in a way that fosters collaboration amongst the variety of stakeholders

Again– GitHub will be the primary hub for discussion and collaboration

Thank you for your participation so far!

	Last 2 Weeks	Total
Individual Discussions	6	23
Top Level Comments	19	123
Comment replies	19	193

Top 5 authors from the last two weeks:

- ★ 1. iteuscher
- ★ 2. sfc-gh-schaudhry
- ★ 3. sunstonesecure-robert
- ★ 4. Ethanolivertroy
- ★ 5. brian-ruf

https://github.com/FedRAMP/automating-assessment-cwg/discussions

Ideas, themes, and code!

- An example of automating continuous monitoring of Continuous Monitoring and High Availability using containers and kubernetes.
- Using MCP servers provided by cloud hosts to automatically validate secure configurations.
- “Identify the discrete underlying facts that define controls, then automate the checking of those key facts, avoiding unnecessary excess verbiage in the control language.”
- KSI-3IR-5 Implement zero trust design principles

20x Phase One Pilot Deliverables

- *Summary of the Cloud Service Provider and Cloud Service Offering*
- *Rationale for the approach used to generate the submission*
- *Summary from a 3PAO explaining their assessment approach*
- *Machine-readable assessment file, in a format of your choice*
  - *Include the status of each KSI, supporting evidence, and integrated verification by a 3PAO*
  - *Include a data definition or data schema*
  - *Should use only printable ASCII and graphical Unicode characters*
- *A proposal or prototype for continuously reporting*

This is the most flexible phase– Phase One submissions will serve as examples to the community and inform future standards for future phases

Phase One Pilot Draft Submissions

- FedRAMP will begin accepting draft submissions between May 19th and May 25th
  - They do not have to be finalized or even completed
  - May contain placeholder or anonymized data
- We will not provide individual feedback for non-public submissions
  - We will review and share generalized public feedback

Please post your draft submission publicly.

Final Pilot Submissions

- Final submission window will open after May 30th, and will remain open based on demand
- **Our strong preference is that you submit your package publicly**
  - Self-hosted or hosted on a publicly available website
  - Does not require an account/login
  - No Terms of Service, NDAs, etc.

https://www.fedramp.gov/20x/phase-one/

Alternative Final Pilot Submissions

- We started a new discussion thread in the forum to solicit ideas and/or challenges for public submission.
  - If you have concerns or questions, post them there
- We are still exploring alternative methods, but here are our constraints:
  - No emails with large attachments
  - No login details (we do not want to manage accounts)
  - No compiled binaries or installations
  - No required NDA or ToS

Community Working Groups

We have a new category of discussion in our working groups called “20x Phase One Pilot”. This category is present in:

Automating Assessment

Discuss auto-generated evidence and machine-readable data formats here

Applying Existing Frameworks

Discuss applying SOC 2 audits & other certs to the FedRAMP 20x KSIs here

Continuous Reporting

Discuss prototypes and proposals for reporting continuously here

fedramp.gov/20x/working-groups

This week's discussion starters

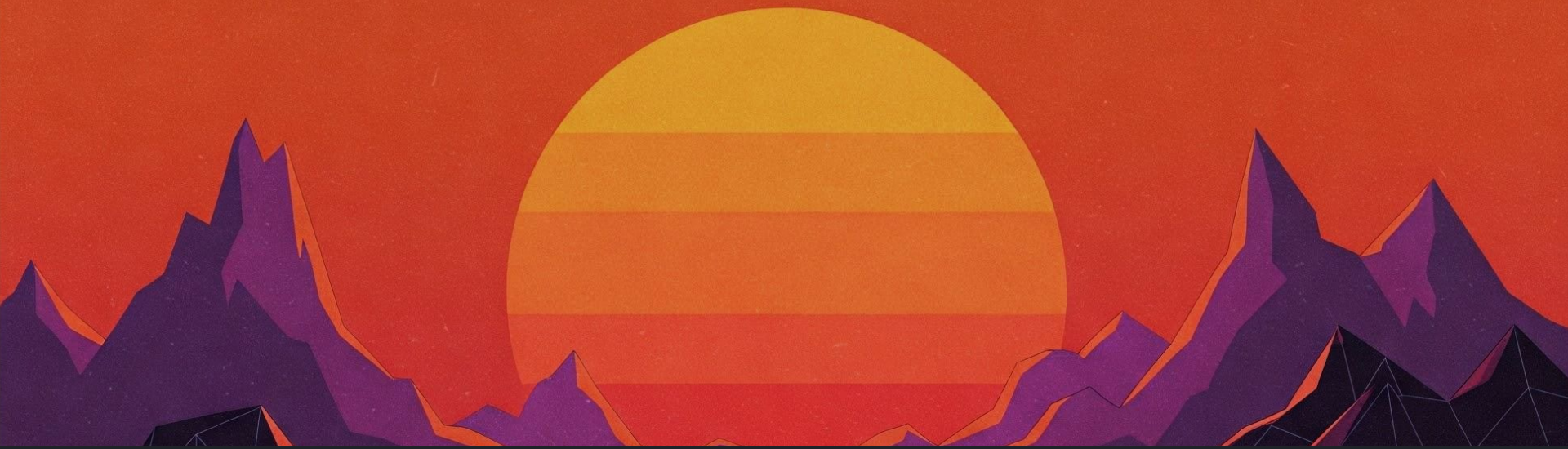
- As previously mentioned, we have a discussion post up about 20x public submission concerns and ideas.
- We are moving on to Secure Configuration, or KSI-SC:
    - **A secure cloud service offering will enforce the use of approved cryptography, continuously verify component integrity, and restrict access to external services.**
        - Which validations are conducive to automation, and which ones are not?
        - What auto-generated evidence can be applied to each validation?
        - How might 3PAOs assess these validations?

You can already engage with these on GitHub!

Working Group Next Steps

- Our next recap will be held on the **28th of May at 1 PM ET.**
- If you are interested in bringing forward a topic, prototype, or idea to this working group, post in the discussion forums
  - **This is NOT an opportunity for product pitches**

Close-out



Automating Assessment Working Group