April, 2025

fedramp.gov/20x

FedRAMP20X

Automating Assessment
Working Group Townhall

Starting at 1:03pm

[REC ●]

Today's Agenda

- How we'll work recap
- GitHub Discussion Recap
- Big themes/questions
- How this is informing our work
- Anatomy of a KSI
- Next steps

Workgroup Discussion Forum on GitHub:

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

How we'll work

For all of our Working Groups:

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

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!

As of yesterday:

- 13 individual discussions
- 84 top level comments
- 135 comment replies
- 60 unique users

Top Individual Contributors:

sunstonesecure-robert
dljenkins
ethanolivertroy
jsantore-cgc
JosephScarzone
kamamanh

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

Ideas, themes, and code!

"We will know our environments better than anyone and know how to build processes and 'Compliance-as-Code' to be able to report on the results for the KSIs. "

"Let's not define metrics that measure artificial things that do not defend against insider or outside threats and failure modes."

"Each CSP offering the object store or database store should provide an API to query the status of the encryption settings as part of the service itself... The 3PAO would only need to validate this one time that it was implemented correctly and thereafter we just enable clients to invoke on-demand or have it invoked as part of a compliance dashboard."

"We could just have a hypothetical endpoint, like GET /fedramp-metrics that 3PAOs can hit and get a JSON response:
a. controlsChecked vs. controlsPassed vs. controlsFailed gives a quick overview
b. Each controlResults[] entry shows a short explanation of pass/fail
c. Linking to a remediationURL provides direct instructions or next steps in a code-friendly (not doc-heavy) manner"

Concerns and questions

"How do we know we can trust the tool to report accurately? It is not sufficient to just say 'ok, my monitoring agent says that control X is good' without understanding what the agent is checking."

"How would you verify that the tool collecting evidence isn't just generating a compliant-looking report? We need a way to ensure the authenticity of automated evidence collection."

"Not all CSPs are currently using third-party GRC tools due to the cost that comes with those tools."

"The more complex you make the system, the more things you have to scan, STIG, patch, pay usage for, etc.

"How do we ensure that automated checks truly capture the full scope of security requirements, especially for complex, multi-faceted environments?"

How this is informing FedRAMP's work

- We hear your ideas!
  - Dynamic KSIs with flexibility in implementation
  - Configs from Iaas/PaaS/GRC providers, assessed once and then reused
  - Cryptographic evidence verification
  - These ideas are factoring into our overall strategy.

- We also hear your concerns!
  - Increased cost and complexity for CSPs
  - How can we ensure information can be trusted?

- Because of this, **we are drafting Low Impact Key Security Indicators**
  - Starting small means we can delay concerns about large, complex systems
  - Everyone will have an opportunity to provide **official feedback** on our drafts via the RFC process.

How this will affect the CWG's engagement

In the near to medium term, the automating assessment CWG will focus on cross-platform, trusted technical validation for the KSIs

- How could that engagement look?
  - Prototype development
  - Implementation ideas for specific platforms
  - Example output and/or data from platforms, GRC tools, etc
  - Discussion around KSIs that are not automation friendly, and how to validate them.

Let’s start with controls.

- **Multiple controls** across different control families **address the same risk**
  - I.e. the “related controls” list in 800-53

- **Incident response according to 800-53**
  - Obviously, all the IR controls
  - But also: RA-3, RA-5, SI-2, CP-2, CP-10, CP-9, PS-8

- **Addressing all of these NIST controls is hard.**
  - Lots of rework
  - Lots of documentation/narrative
  - Lots of reading for the PMO

Anatomy of a KSI

- **Incident response KSI**
  - Risk: External factors can impact the security of the system.
  - Security Practices or Objectives:
    - Evaluate risk continuously
    - Plan for unanticipated events
    - Address incidents promptly and effectively

1. When building a KSI we start by looking at a particular risk factor.
2. Next we list some security best practices and objectives that help reduce the risk factor
3. The final KSI will describe the practices and objectives we want the CSP to demonstrate.
4. The CSP will provide evidence demonstrating how they achieve the KSI objectives.
5. Some KSIs will include specific statutory or regulatory requirements that must be asserted

CSP Validations

Each KSI will give the CSP the opportunity to provide data points to demonstrate their capability in achieving the desired security objective. The CSP will “validate” that each data point is accurate and will provide evidence to support the validation.

Validation	Evidence could include
Enforce phishing-resistant multi-factor authentication (MFA)	IDM service verification that all accounts require MFA and the type of MFA used
Use secure API authentication methods	Key Management System (KMS) configuration
Use a least-privileged, role-based security model.	SOC II or 3PAO report

CSP can add as many examples/data points as they wish. Demonstrate to your customers your value proposition

This week’s discussion starters

- Before the official draft of KSIs are out, we want to **focus in on 2 sample validations**
  - How might a small Li-SaaS company report these specifically?
  - How do we automate these on every major platform right now?
  - How do we create processes that allow 3PAOs to verify it?
- We will start with an easy one and a hard one:
  - **Multi-Factor Authentication: How do we ensure that phishing resistant MFA is enabled for users?**
  - **Change Management: How do we monitor system changes and ensure impacts to security are measured and addressed?**

You can already find the discussion posts up on GitHub!

Working Group Next Steps

- Our next recap will be held on **30 April at 1 PM EST.**

- If you are interested in bringing forward a topic, prototype, or idea to this working group, post in the discussion forums

    - **<u>This is NOT an opportunity for product pitches</u>**

Close-out